



GGSN Administration Guide, StarOS Release 21.4

First Published: 2017-10-26

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

About this Guide xxxvii

Conventions Used xxxvii

Supported Documents and Resources xxxviii

Related Common Documentation xxxviii

Related Product Documentation xxxviii

Obtaining Documentation xxxix

Contacting Customer Support xxxix

CHAPTER 1

GGSN Support in GPRS/UMTS Wireless Data Services 1

Product Description 1

Product Specification 2

Licenses 2

Qualified Platforms 2

Operating System Requirements 3

Network Deployment and Interfaces 3

GGSN in the GPRS/UMTS Data Network 4

Supported Interfaces 5

Features and Functionality - Base Software 8

16,000 SGSN Support 8

AAA Server Groups 8

Access Control List Support 9

ANSI T1.276 Compliance 9

APN Support 10

APN AMBR Support 11

Backup and Recovery of Key KPI Statistics 11

Bulk Statistics Support 12

Direct Tunnel Support 13

DHCP Support	14
DHCPv6 Support	15
DHCPv6 Prefix Delegation	16
DSCP Marking	16
IMS Emergency Session Support	16
Framed-Route Attribute Support	17
Generic Corporate APN	17
GnGp Handoff Support	17
GTPP Support	18
Host Route Advertisement	19
IP Policy Forwarding	20
IP Header Compression - Van Jacobson	20
IPv6 Support	21
MPLS Forwarding with LDP	22
Overlapping IP Address Pool Support	23
PDP Context Support	23
Per APN Configuration to Swap out Gn to Gi APN in CDRs	24
Peer GTP Node Profile Configuration Support	24
Port Insensitive Rule for Enhanced Charging Service	25
P-CSCF Discovery Support	25
Quality of Service Support	26
RADIUS Support	26
RADIUS VLAN Support	28
Routing Protocol Support	28
Subscriber Session Trace Support	30
Support of Charging Characteristics Provided by AAA Server	31
Support of all GGSN generated causes for partial G-CDR closure	31
Support of ULI/RAI Generation	32
Threshold Crossing Alerts (TCA) Support	32
Virtual APN Selection	33
Features and Functionality - Optional Enhanced Feature Software	33
Common Gateway Access Support	33
Dynamic RADIUS Extensions (Change of Authorization)	34
GRE Protocol Interface Support	34
GTP Throttling	35

Bypass Rate Limit Function	36
Gx Interface Support	37
Inter-Chassis Session Recovery	38
IP Security (IPSec)	39
IPNE Service Support	39
IPv6 Prefix Delegation from the RADIUS Server and the Local Pool	39
L2TP LAC Support	40
L2TP LNS Support	40
Lawful Intercept	41
Mobile IP Home and Foreign Agents	42
Mobile IP NAT Traversal	43
NEMO Service Support	43
Multimedia Broadcast Multicast Services Support	43
Overcharging Protection on Loss of Coverage	44
Proxy Mobile IP	44
Session Persistence	45
Session Recovery Support	46
Traffic Policing and Rate Limiting	46
User Location Change Reporting Support	48
3GPP ULI Reporting Support Enhanced	48
Feature Change	48
How GGSN Works	50
PDP Context Processing	50
Dynamic IP Address Assignment	51
Subscriber Session Call Flows	52
Transparent Session IP Call Flow	54
Non-Transparent IP Session Call Flow	55
Network-Initiated Session Call Flow	57
PPP Direct Access Call Flow	58
Virtual Dialup Access Call Flow	60
Corporate IP VPN Connectivity Call Flow	61
Mobile IP Call Flow	63
Proxy Mobile IP Call Flows	66
IPv6 Stateless Address Auto Configuration Flows	68
Supported Standards	69

3GPP References	69
IETF References	70
Object Management Group (OMG) Standards	73

CHAPTER 2

Understanding the Service Operation 75

Terminology	75
Contexts	76
Logical Interfaces	77
Bindings	78
Services	79
How the System Selects Contexts	80
Context Selection for Subscriber Sessions	81

CHAPTER 3

GGSN Service Configuration Procedures 83

GGSN Service Configuration	84
GGSN Service Creation and Binding	84
Accounting Context and Charging Characteristics Configuration	85
SGSN and PLMN Policy Configuration	85
Network-requested PDP Context Support Configuration	86
GGSN Configuration Verification	86
GTPP Accounting Support Configuration	87
GTPP Group Creation	88
GTPP Group Configuration	89
GTPP Group Configuration Verification	90
APN Configuration	90
APN Creation and Configuration	91
Authentication, Accounting, and GTPP Group Configuration in APN	92
Authentication and Accounting Configuration in APN	92
GTPP Group Association to APN	92
IP Address Allocation Method Configuration in APN	92
Charging Characteristics Parameter Configuration in APN	93
Virtual APN Configuration	94
Other Optional Parameter Configuration in APN	94
APN Configuration Verification	95
DHCP Service Configuration	96

DHCP Service Creation	97
DHCP Server Parameter Configuration	97
DHCP Service Configuration Verification	98
DHCPv6 Service Configuration	99
DHCPv6 Service Creation	99
DHCPv6 Server Parameter Configuration	100
DHCPv6 Client Parameter Configuration	100
DHCPv6 Profile Configuration	101
Associate DHCPv6 Configuration	102
DHCPv6 Service Configuration Verification	102
DNS Configuration for IPv4v6 PDP Context	103
Creating IPv4/IPv6 DNS List	103
Configuring IPv4 DNS	104
Configuring IPv6 DNS	104
IP Address Pool Configuration on the System	104
IPv4 Pool Creation	106
IPv6 Pool Creation	106
IP Pool Configuration Verification	107
Gn-Gp Handoff Support Configuration	107
GTP-U Service Configuration	108
Modifying GGSN Configuration for Gn-Gp Handoff	108
APN Configuration for Gn-Gp Handoff	109
Gn-Gp Configuration Verification	109
FA Services Configuration	110
FA Service Creation	110
IP Interface and UDP Port Binding for Pi Interface	111
Security Parameter Index (SPI) Configuration	111
FA Agent Advertisement Parameter Configuration	112
Subscriber Registration, Authentication and Timeout Parameter Configuration	113
Revocation Message Configuration	113
FA Service Configuration Verification	114
Common Gateway Access Support Configuration	114
Diameter End-Point Configuration	115
AAA Group Configuration	115
Authorization over S6b Configuration	116

DNS Client Configuration	116
Duplicate Call Accept Configuration	116
Common Gateway Access Support Configuration Verification	117
Rf Interface Configuration for Offline Charging	117
Accounting Policy Configuration	118
Diameter End-Point Configuration	118
AAA Group Configuration	118
APN Configuration for Rf Interface	118
Rf Interface Configuration Verification	119
Configuring RFL Bypass Feature	119
Configuring the Throttling Override Policy Mode	119
Configuring the RLF Bypass Feature	120

CHAPTER 4

GGSN Configuration Example 121

Information Required	122
Source Context Configuration	123
Destination Context Configuration	127
How This Configuration Works	132
Transparent IP PDP Context Processing	133
Non-transparent IP PDP Context Processing	134
PPP PDP Context Processing	135
Network-requested PDP Context Processing	136

CHAPTER 5

Mobile IP Configuration Examples 139

Example 1: Mobile IP Support Using the System as a GGSN/FA	139
Information Required	140
Source Context Configuration	140
AAA Context Configuration	144
Mobile IP Destination Context Configuration	148
Optional Destination Context Configuration	150
How This Configuration Works	151
Example 2: Mobile IP Support Using the System as an HA	152
Information Required	153
Source Context Configuration	153
Destination Context Configuration	158

How This Configuration Works 159

Example 3: HA Using a Single Source Context and Multiple Outsourced Destination

Contexts 160

Information Required 161

Source Context Configuration 161

Destination Context Configuration 165

System-Level AAA Configuration 168

How This Configuration Works 170

CHAPTER 6

GGSN and Mobile IP Service in a Single System Configuration Example 173

Using the System as Both a GGSN/FA and an HA 173

Information Required 174

Source Context Configuration 175

Destination Context Configuration 179

Mobile IP Destination Context Configuration 185

How This Configuration Works 189

CHAPTER 7

Mobile-IP and Proxy-MIP Timer Considerations 193

Call Flow Summary 193

Dealing with the 'Requested Lifetime Too Long' Error Code 195

Controlling the Mobile IP Lifetime on a Per-Domain Basis 195

CHAPTER 8

Session Tracing 199

Session Tracing Overview 199

Session Trace Types 201

Session Trace Activation 202

Session Trace Deactivation 202

Data Collection 202

Data Forwarding 203

Supported Standards 203

Configuring Session Trace Functionality 203

Enabling Session Tracing 204

Verifying that Session Tracing is Enabled 205

Disabling Session Trace Functionality 205

Configuring a Session Trace Template for the Management Trace Function 205

Verifying the Session Trace Template Configuration	209
Disabling the Session Trace Template Configuration	209
Disabling the Session Trace Template Configuration per Network Element and Subscriber	209
Configuring a Management Session Trace	209
Verifying the Management Trace Configuration	210
Disabling the Management Trace Configuration	210
Configuring a Signaling Session Trace	210
Verifying the Signaling Session Trace Configuration	211
Disabling the Signaling Session Trace	211
Configuring a Random Trace	211
Verifying the Random Trace Configuration	214
Disabling the Random Trace for a Specific Network Element	214
Monitoring the Session Trace Functionality	215
Supported SAEGW Session Trace Configurations	215
Session Trace File Example	219

CHAPTER 9
Troubleshooting the Service 223

Test Commands	223
Using the PPP Echo-Test Command	223
Using the GTPC Test Echo Command	224
Using the GTPU Test Echo Command	224
Using the GTPv0 Test Echo Command	225
Using the DHCP Test Command	226
Testing GTPP Accounting with a CGF	226
Testing GTPP Connectivity with a GSS	227

CHAPTER 10
3GPP ULI Reporting Support Enhanced 229

Feature Change	229
----------------	-----

CHAPTER 11
Backup and Recovery of Key KPI Statistics 231

Feature Description	231
How It Works	231
Architecture	232
Limitations	233

Configuring Backup Statistics Feature	233
Configuration	233
Verifying the Backup Statistics Feature Configuration	234

CHAPTER 12

Bulkstats for Average Data Rate per IPPOOL	235
Feature Summary and Revision History	235
Feature Description	236
Monitoring and Troubleshooting	236
Bulk Statistics	236
Datarate-IPPool Schema	236
Show Commands and/or Outputs	236
show bulkstats schemas	236
show bulkstats data	237
show subscribers data-rate ip-pool <pool_name>	237

CHAPTER 13

CoA, RADIUS DM, and Session Redirection (Hotlining)	239
RADIUS Change of Authorization and Disconnect Message	239
CoA Overview	239
DM Overview	240
License Requirements	240
Enabling CoA and DM	240
Enabling CoA and DM	240
CoA and DM Attributes	241
CoA and DM Error-Cause Attribute	242
Viewing CoA and DM Statistics	243
Session Redirection (Hotlining)	244
Overview	244
License Requirements	244
Operation	244
ACL Rule	244
Redirecting Subscriber Sessions	244
Session Limits On Redirection	245
Stopping Redirection	245
Handling IP Fragments	245
Recovery	245

AAA Accounting 245

Viewing the Redirected Session Entries for a Subscriber 246

CHAPTER 14

Direct Tunnel for 4G (LTE) Networks 249

Direct Tunnel for 4G Networks - Feature Description 249

How It Works 252

DT Establishment Logic 253

Establishment of Direct Tunnel 254

Direct Tunnel Activation for Primary PDP Context 255

Direct Tunnel Activation for UE Initiated Secondary PDP Context 255

RAB Release with Direct Tunnel 256

Iu Release with Direct Tunnel 257

Service Request with Direct Tunnel 258

Downlink Data Notification with Direct Tunnel when UE in Connected State 259

Downlink Data Notification with Direct Tunnel when UE in Idle State 260

Intra SGSN Routing Area Update without SGW Change 262

Routing Area Update with S-GW Change 265

Intra SRNS with S-GW Change 268

Intra SRNS without S-GW Change 270

New SRNS with S-GW Change and Direct Data Transfer 271

New SRNS with S-GW Change and Indirect Data Transfer 273

Old SRNS with Direct Data Transfer 275

Old SRNS with Indirect Data Transfer 276

Network Initiated Secondary PDP Context Activation 278

PGW Init Modification when UE is Idle 278

Limitations 279

Standards Compliance 280

Configuring Support for Direct Tunnel 280

Configuring Direct Tunnel on an S4-SGSN 280

Enabling Setup of GTP-U Direct Tunnel 280

Enabling Direct Tunnel to RNCs 281

Restricting Direct Tunnels 282

Verifying the Call-Control Profile Configuration 282

Verifying the RNC Configuration 282

Configuring S12 Direct Tunnel Support on the S-GW 283

Monitoring and Troubleshooting Direct Tunnel 283

show subscribers sgsn-only 283

show gmm-sm statistics sm-only 284

Direct Tunnel Bulk Statistics 284

CHAPTER 15

Embed IMSI into Session Id 285

Feature Summary and Revision History 285

Feature Description 286

How It Works 286

Limitations 287

Configuring Diameter Accounting Interim Interval 287

Monitoring and Troubleshooting 288

Show Commands and Outputs 288

show configuration 288

show configuration [verbose] 288

CHAPTER 16

Extended QCI Options 289

Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters 289

Feature Description 289

Configuring ARP Granularity for QCI Level Counters 290

Create a Stats Profile 290

Enable the Collection of Packet Drop Statistics 291

Enable the Collection of QCI/ARP Level Statistics 291

Associate a Stats Profile with an APN 292

Verify the Configuration 292

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters 293

Bulk Statistics 293

APN Schema 293

Show Commands 294

show apn statistics 294

show configuration 301

show stats-profile name 301

DSCP Marking Based on Both QCI and ARP Values 301

Feature Description 301

Relationships to Other Features 302

Licensing	302
How It Works	302
Configuring DSCP Marking Based on Both QCI and ARP Values	303
Configuring QCI-QoS Mapping	303
Associating QCI-QoS Mapping Configuration	303
Configuring CS5 Marking for GTP-C	304
Verifying the Configuration	304
Monitoring DSCP Marking Based on Both QCI and ARP Values	304
Output of Show Commands	304
show qci-qos-mapping table all	304
New Standard QCI Support	304
Feature Description	305
Licensing	305
How it Works	305
Expected Call Flow Output	306
New Call Procedure	306
Handoff Procedures	307
UE Initiated Bearer Creation	313
Bearer Creation	313
Bearer Update	314
Configuring New Standard QCIs	314
Configuring QCI-QoS Mapping	314
Configuring Local QCI Mapping for Gn/Gp QoS Support	315
Configuring Transaction Rate Network Initiated Setup/Teardown Events	315
Enable Mission Critical QCIs	316
Verifying the Configuration	316
Monitoring the Feature	316
Bulk Statistics	316
APN Schema	317
GTPU Schema	318
P-GW Schema	318
SAEGW Schema	319
S-GW Schema	325
System Schema	330
Show Commands	331

- show apn statistics all 331
- show gtpu statistics 332
- show pgw-service statistics all verbose 332
- show saegw-service statistics all verbose 333
- show sgw-service statistics all verbose 334

Non-standard QCI Support 338

Feature Description 338

- Licensing 338

How It Works 338

- Limitations 339

- Standards Compliance 339

Configuring Non-standard QCI Support 339

- Configuring Non-standard QCI Support in P-GW 339

Monitoring Non-standard QCI Support 340

- Bulk Statistics 340

- APN Schema 340

Output of Show Commands 341

- show apn statistics 341
- show qci-qos-mapping table all 341

CHAPTER 17

GGSN UPC Collision Handling 343

GGSN UPC Collision Handling 343

Feature Description 343

How It Works 343

Limitations 344

Configuring GGSN UPC Collision Handling 344

- gtpc handle-collision 344

- Verifying the Configuration 345

Monitoring and Troubleshooting GGSN UPC Collision Handling 345

Show Commands for GGSN UPC Collision Handling 346

- show configuration 346
- show configuration verbose 346
- show ggsn-service name service_name 346
- show gtpc statistics 346
- show gtpc statistics [format1 | ggsn-service service_name | verbose] 347

CHAPTER 18**GRE Protocol Interface 349**

- Introduction 350
- Supported Standards 351
- Supported Networks and Platforms 351
- Licenses 351
- Services and Application on GRE Interface 351
- How GRE Interface Support Works 351
 - Ingress Packet Processing on GRE Interface 351
 - Egress Packet Processing on GRE Interface 354
- GRE Interface Configuration 355
 - Virtual Routing And Forwarding (VRF) Configuration 356
 - GRE Tunnel Interface Configuration 357
 - Enabling OSPF for VRF 357
 - Associating IP Pool and AAA Group with VRF 358
 - Associating APN with VRF 358
 - Static Route Configuration 359
 - Verifying Your Configuration 359

CHAPTER 19**Gx Interface Support 361**

- Rel. 7 Gx Interface 361
 - Introduction 362
 - Supported Networks and Platforms 364
 - License Requirements 364
 - Supported Standards 364
 - Terminology and Definitions 365
 - Policy Control 365
 - Charging Control 369
 - Charging Correlation 370
 - Policy and Charging Control (PCC) Rules 370
 - PCC Procedures over Gx Reference Point 372
 - Request for PCC Rules 372
 - Provisioning of PCC Rules 372
 - Selecting a PCC Rule for Uplink IP Packets 373
 - Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets 374

Volume Reporting Over Gx	374
License Requirements	374
Supported Standards	375
Feature Overview	375
Usage Monitoring	376
Usage Reporting	377
ICSR Support for Volume Reporting over Gx (VoRoGx)	379
How Rel. 7 Gx Works	379
Configuring Rel. 7 Gx Interface	382
Configuring IMS Authorization Service at Context Level	383
Verifying the Configuration	385
Applying IMS Authorization Service to an APN	385
Verifying Subscriber Configuration	386
Configuring Volume Reporting over Gx	386
Gathering Statistics	387
Rel. 8 Gx Interface	388
HA/PDSN Rel. 8 Gx Interface Support	388
Introduction	389
License Requirements	391
Supported Standards	391
Terminology and Definitions	391
Policy Control	392
Binding	392
Gating Control	392
Event Reporting	392
QoS Control	392
Other Features	393
PCC Rule Error Handling	393
Time of the Day Procedures	394
Support for Firewall Policy on Gx	394
Charging Control	394
Charging Correlation	395
Policy and Charging Control (PCC) Rules	395
PCC Procedures over Gx Reference Point	397
Request for PCC Rules	397

Provisioning of PCC Rules	397
Selecting a PCC Rule for Uplink IP Packets	398
Selecting a PCC Rule for Downlink IP Packets	398
How it Works	398
Configuring HA/PDSN Rel. 8 Gx Interface Support	402
Configuring IMS Authorization Service at Context Level	403
Verifying the IMSA Service Configuration	404
Applying IMS Authorization Service to Subscriber Template	404
Verifying the Subscriber Configuration	404
Gathering Statistics	405
P-GW Rel. 8 Gx Interface Support	406
Introduction	406
Terminology and Definitions	406
Volume Reporting Over Gx	406
License Requirements	406
Supported Standards	406
Feature Overview	407
Usage Monitoring	407
Usage Reporting	409
ICSR Support for Volume Reporting over Gx (VoRoGx)	410
Rel. 9 Gx Interface	411
P-GW Rel. 9 Gx Interface Support	411
Introduction	411
Terminology and Definitions	411
Volume Reporting Over Gx	412
License Requirements	412
Supported Standards	412
Feature Overview	412
Usage Monitoring	413
Usage Reporting	414
ICSR Support for Volume Reporting over Gx (VoRoGx)	416
3GPP Rel.9 Compliance for IPFilterRule	416
Feature Description	416
Configuring Rel.9 Compliant AVPs	417
Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule	418

Rel. 10 Gx Interface	419
P-GW Rel. 10 Gx Interface Support	419
Introduction	419
Terminology and Definitions	420
Volume Reporting Over Gx	420
License Requirements	420
Supported Standards	420
Feature Overview	420
Usage Monitoring	421
Usage Reporting	422
ICSR Support for Volume Reporting over Gx (VoRoGx)	424
Use of the Supported-Features AVP on the Gx Interface	424
Rule-Failure-Code AVP	426
Sponsored Data Connectivity	426
Volume Reporting	427
Supported Gx Features	427
Assume Positive for Gx	427
Default Policy on CCR-I Failure	428
Gx Back off Functionality	429
Support for Volume Reporting in Local Policy	429
Support for Session Recovery and Session Synchronization	430
Configuring Gx Assume Positive Feature	431
Configuring Local Policy Service at Global Configuration Level	431
Configuring Failure Handling Template at Global Configuration Level	432
Associating Local Policy Service and Failure Handling Template	432
Verifying Local Policy Service Configuration	432
Time Reporting Over Gx	432
License Requirements	433
Feature Overview	433
Limitations	433
Usage Monitoring	434
Usage Monitoring at Session Level	434
Usage Monitoring at Flow Level	434
Usage Monitoring for Predefined and Static Rules	434
Usage Monitoring for Dynamic Ruledefs	434

Usage Reporting	434
Configuring Time Reporting over Gx	435
Support for Multiple Active and Standby Gx Interfaces to PCRF	436
Configuring Diameter Peer Selection at Diabase in Failure Scenarios	437
Support for Multiple CCR-Us over Gx Interface	437
Configuring Gateway Node to Support Back-to-Back CCR-Us	438
Support for RAN/NAS Cause IE on Gx Interface	439
Configuring Supported Feature Netloc-RAN-NAS-Cause	439
Support ADC Rules over Gx Interface	439
Limitations	440
Configuring ADC Rules over Gx	441
GoR Name Support in TDF-Application-Identifier	441
ADC Mute Customization	442
Enhancement to the ADC Custom Mute/Unmute Functionality	443
Feature Information	443
Feature Changes	444
Limitations	444
How it Works	444
Configuring the ADC Notifications	445
Support for TAI and ECGI Change Reporting	445
Feature Description	445
How it Works	446
Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature	447
Location Based Local-Policy Rule Enforcement	448
Feature Description	448
How it Works	449
Configuring Location Based Local Policy Rule Enforcement Feature	450
Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature	452
Gx Support for GTP based S2a/S2b	453
Gx-based Virtual APN Selection	453
Feature Description	453
Overview	453
License Requirements	454
Limitations	454
Configuring Gx based Virtual APN Selection Feature	454

Verifying the Gx based Virtual APN Configuration	454
Monitoring and Troubleshooting the Gx based Virtual APN Selection	455
show ims-authorization policy-control statistics	455
Debugging Statistics	455
Bulk Statistics for Gx based Virtual APN Selection Feature	455
IMSA Schema	455
System Schema	455
Graceful Handling of RAR from Different Peers	455
NetLoc Feature Enhancement	456
Feature Description	456
Limitations	460
Command Changes	460
gtp-attribute	460
Performance Indicator Changes	461
show configuration	461
show gtp group name group_name	461
RAN-NAS Cause Code Feature Enhancement	461
Feature Description	462
Limitations	464
Command Changes	465
diameter encode-supported-features netloc netloc-ran-nas-cause	465
Session Disconnect During Diamproxy-Session ID Mismatch	466
Feature Description	466
Configuring System to Delete Diamproxy-Session ID Mismatched Sessions	466
Monitoring and Troubleshooting the Mismatched Session Deletion Feature	467
Support for Negotiating Mission Critical QCIs	468
Feature Description	468
Configuring DPCA for Negotiating Mission Critical QCIs	469
Monitoring and Troubleshooting the Mission Critical QCI	469
HSS and PCRF-based P-CSCF Restoration Support for WLAN	470
Feature Description	470
Configuring the HSS/PCRF-based P-CSCF Restoration	471
Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration	473
Loop Prevention for Dynamic Rules	474
Feature Information	474

Feature Description	475
How It Works	475
Configuring Loop Prevention for Dynamic Rules	475
Enabling ACS Policy to Control Loop Prevention	476
Monitoring and Troubleshooting	476
Show Commands and Outputs	476
show active-charging service all	476
show active-charging subscribers full all	476
show active-charging subsystem all	477
Separation of Accounting Interim Interval Timer for RADIUS and Diameter Rf	477
Feature Information	477
Feature Description	478
How It Works	478
Limitations	479
Configuring Diameter Accounting Interim Interval	479
Monitoring and Troubleshooting	480
Show Commands and Outputs	480
show aaa group { name <group_name> all }	480
show configuration [verbose]	480
Enhancement to OCS Failure Reporting for Gy	481
Feature Information	481
Feature Description	481
Support Added for RAN/NAS Cause Code for S5/S8 and S2b Interfaces	482
Feature Information	482
Feature Changes	483
Limitations	486
Command Changes	486
diameter encode-supported-features netloc-ran-nas-cause	486

CHAPTER 20
Gy Interface Support 487

Introduction	487
License Requirements	489
Supported Standards	489
Features and Terminology	489
Charging Scenarios	489

Session Charging with Reservation	489
Decentralized Unit Determination and Centralized Rating	489
Centralized Unit Determination and Centralized Rating	489
Decentralized Unit Determination and Decentralized Rating	490
Basic Operations	490
Re-authorization	491
Threshold based Re-authorization Triggers	491
Termination Action	491
Diameter Base Protocol	491
Diameter Credit Control Application	492
Quota Behavior	492
Time Quotas	492
Volume Quota	494
Units Quota	494
Granting Quota	494
Requesting Quota	495
Reporting Quota	495
Default Quota Handling	496
Thresholds	496
Conditions for Reauthorization of Quota	497
Discarding or Allowing or Buffering Traffic to Flow	497
Procedures for Consumption of Time Quota	497
Envelope Reporting	498
Credit Control Request	498
Tx Timer Expiry Behavior	500
Redirection	500
Triggers	501
Tariff Time Change	501
Final Unit Indication	502
Final Unit Indication at Command Level	502
Final Unit Indication at MSCC Level	502
Credit Control Failure Handling	502
CCFH with Failover Supported	502
CCFH with Failover Not Supported	503
Failover Support	503

Recovery Mechanisms	504
Error Mechanisms	504
Unsupported AVPs	504
Invalid Answer from Server	504
Result Code Behavior	504
Supported AVPs	505
Unsupported AVPs	508
PLMN and Time Zone Reporting	514
Interworking between Session-based Gy and Event-based Gy	515
OCS Unreachable Failure Handling Feature	515
Enhancement to OCS Failure Reporting for Gy	517
Feature Description	517
Backpressure Handling	518
Gy Backpressure Enhancement	518
Gy Support for GTP based S2a/S2b	519
Generating OOC/ROC with Changing Association between Rule and RG	519
Static Rulebase for CCR	519
CC based Selective Gy Session Control	520
Feature Description	520
Relationships to Other Features	521
Limitations	521
Configuring CC based Selective Gy Session Control	521
Configuring CC Value	521
Verifying the Selective Gy Session Control Configuration	522
Monitoring and Troubleshooting the Selective Gy Session Control Feature	522
show active-charging sessions	522
Credit-Control Group in Rulebase Configuration	522
Feature Description	522
Configuring Credit-Control Group in Rulebase	523
Monitoring and Troubleshooting the CC-Group Selection in Rulebase	524
Combined CCR-U Triggering for QoS Change Scenarios	524
Re-activating Offline Gy Session after Failure	525
Feature Description	525
Limitations and Restrictions	525
Configuring Offline Gy Session after Failure	526

Monitoring and Troubleshooting the Offline Gy Session after Failure	527
Suppress AVPs	527
Feature Description	527
Command Changes	527
suppress_avp	527
Performance Indicator Changes	528
show configuration	528
Configuring Gy Interface Support	529
Configuring GGSN / P-GW / IPSG Gy Interface Support	529
Configuring HA / PDSN Gy Interface Support	530
Configuring PLMN and Time Zone Reporting	531
Configuring Server Unreachable Feature	532
Configuring Static Rulebase for CCR	533
Configuring Gy for GTP based S2a/S2b	533
Gathering Statistics	533

CHAPTER 21

ICAP Interface Support 535

ICAP Interface Support Overview	535
Supported Networks and Platforms	537
License Requirements	537
Failure Action on Retransmitted Packets	537
ICAP Client Communication with RFC 3507 compliance	538
Configuring ICAP Interface Support	540
Creating ICAP Server Group and Address Binding	541
Configuring ICAP Server and Other Parameters	541
Configuring ECS Rulebase for ICAP Server Group	542
Configuring Charging Action for ICAP Server Group	543
Verifying the ICAP Server Group Configuration	543

CHAPTER 22

IP Header Compression 545

Overview	545
Configuring VJ Header Compression for PPP	546
Enabling VJ Header Compression	547
Verifying the VJ Header Compression Configuration	547
Configuring RoHC Header Compression for PPP	547

Enabling RoHC Header Compression for PPP	548
Verifying the Header Compression Configuration	548
Configuring Both RoHC and VJ Header Compression	549
Enabling RoHC and VJ Header Compression for PPP	549
Verifying the Header Compression Configuration	550
Configuring RoHC for Use with SO67 in PDSN or HSGW Service	550
Enabling RoHC Header Compression with PDSN	550
Enabling RoHC Header Compression with HSGW	551
Verifying the Header Compression Configuration	551
Using an RoHC Profile for Subscriber Sessions	552
Creating RoHC Profile for Subscriber using Compression Mode	552
Creating RoHC Profile for Subscriber using Decompression Mode	553
Applying RoHC Profile to a Subscriber	553
Verifying the Header Compression Configuration	554
Disabling VJ Header Compression Over PPP	554
Disabling VJ Header Compression	555
Verifying the VJ Header Compression Configuration	555
Disabling RoHC Header Compression Over SO67	555
Disabling RoHC Header Compression	556
Verifying the Header Compression Configuration	556
Checking IP Header Compression Statistics	556
RADIUS Attributes for IP Header Compression	557

CHAPTER 23

IP Pool Sharing Protocol 559

Overview	559
Primary HA Functionality	560
Secondary HA Functionality	560
Requirements, Limitations, & Behavior	560
How IPSP Works	561
IPSP Operation for New Sessions	562
IPSP Operation for Session Handoffs	563
Configuring IPSP Before the Software Upgrade	564
Configuring the AAA Server for IPSP	564
Enabling IPSP on the Secondary HA	565
Enabling IPSP on the Primary HA	565

Verifying the IPSP Configuration	566
Configuring IPSP After the Software Upgrade	566
Disabling IPSP	567

CHAPTER 24

IPv6 Prefix Delegation from the RADIUS Server and the Local Pool 569

Feature Description	569
IPv6 Prefix Delegation from the RADIUS Server	569
How It Works	570
Configuring APN to Enable Prefix Delegation From RADIUS Server	572
Verifying Prefix Delegation from the RADIUS Server	572
show dhcpv6 statistics	572
show sub ggsn-only full all	573
show sub pgw-only full all	573
show sub saegw-only full all	574
IPv6 Prefix Delegation from the Local Pool	574
How It Works	574
Configuring APN to Enable Prefix Delegation From Local Pool	575
Configuration Overview	575
Configuring APN for Private Pool Name	575
Configuring Prefix Delegation on Destination Context	576
Verifying Prefix Delegation from the Local Pool	576
show dhcpv6 statistics	577
show sub ggsn-only full all	577
show sub pgw-only full all	577
show sub saegw-only full all	577
IPv6 Interface ID from the RADIUS Server	578
show apn statistics	578
Limitations	578

CHAPTER 25

L2TP Access Concentrator 579

Applicable Products and Relevant Sections	580
Supported LAC Service Configurations for PDSN Simple IP	581
Attribute-based Tunneling	582
How The Attribute-based L2TP Configuration Works	582
Configuring Attribute-based L2TP Support for PDSN Simple IP	583

PDSN Service-based Compulsory Tunneling	583
How PDSN Service-based Compulsory Tunneling Works	583
Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP	585
Supported LAC Service Configurations for the GGSN and P-GW	586
Transparent IP PDP Context Processing with L2TP Support	587
Non-transparent IP PDP Context Processing with L2TP Support	589
PPP PDP Context Processing with L2TP Support	591
Configuring the GGSN or P-GW to Support L2TP	592
Supported LAC Service Configuration for Mobile IP	592
How The Attribute-based L2TP Configuration for MIP Works	594
Configuring Attribute-based L2TP Support for HA Mobile IP	595
Configuring Subscriber Profiles for L2TP Support	595
RADIUS and Subscriber Profile Attributes Used	595
RADIUS Tagging Support	597
Configuring Local Subscriber Profiles for L2TP Support	597
Configuring Local Subscriber	598
Verifying the L2TP Configuration	599
Tunneling All Subscribers in a Specific Context Without Using RADIUS	
Attributes	599
Configuring LAC Services	599
Configuring LAC Service	600
Configuring LNS Peer	600
Verifying the LAC Service Configuration	601
Modifying PDSN Services for L2TP Support	601
Modifying PDSN Service	602
Verifying the PDSN Service for L2TP Support	602
Modifying APN Templates to Support L2TP	603
Assigning LNS Peer Address in APN Template	603
Configuring Outbound Authentication	604
Verifying the APN Configuration	604

CHAPTER 26
L2TP Network Server 605

LNS Service Operation	605
Information Required	606
Source Context Configuration	606

Destination Context Configuration	610
How This Configuration Works	611
Configuring the System to Support LNS Functionality	612
Creating and Binding LNS Service	613
Configuring Authentication Parameters for LNS Service	613
Configuring Tunnel and Session Parameters for LNS Service	614
Configuring Peer LAC servers for LNS Service	614
Configuring Domain Alias for AAA Subscribers	614
Verifying the LNS Service Configuration	615

CHAPTER 27

Mobile IP Registration Revocation 617

Overview	617
Configuring Registration Revocation	618
Configuring FA Services	619
Configuring HA Services	619

CHAPTER 28

Multimedia Broadcast and Multicast Service 621

Introduction	621
Supported Standards	623
Supported Networks and Platforms	623
Services and Application in MBMS	623
MBMS References and Entities	624
Gmb Reference	624
MBMS UE Context	624
MBMS Bearer Context	625
Broadcast Multicast Service Center (BM-SC)	625
How MBMS Works	625
MBMS Broadcast Mode	625
MBMS Broadcast Mode Procedure	626
MBMS Multicast Mode	626
MBMS Multicast Mode Procedure	627
MBMS Configuration	627
BMSC Profile Configuration	628
MBMS GTPP Configuration	628
MBMS APN Configuration	629

MBMS Provisioning	629
Save the Configuration	629
Managing Your Configuration	629
Gathering MBMS Statistics	631

CHAPTER 29
Multi-Protocol Label Switching (MPLS) Support 633

Overview	633
Chassis as MPLS-CE Connecting to PE	634
Chassis as MPLS-CE Connected to ASBR	635
Engineering Rules	635
Supported Standards	635
Supported Networks and Platforms	636
Licenses	636
Benefits	636
Configuring BGP/MPLS VPN with Static Labels	636
Create VRF with Route-distinguisher and Route-target	637
Set Neighbors and Enable VPNv4 Route Exchange	637
Configure Address Family and Redistributed Connected Routes	638
Configure IP Pools with MPLS Labels	638
Bind DHCP Service for Corporate Servers	638
Bind AAA Group for Corporate Servers	639
Configuring BGP/MPLS VPN with Dynamic Labels	639
Create VRF with Route-distinguisher and Route-target	640
Set Neighbors and Enable VPNv4 Route Exchange	641
Configure Address Family and Redistributed Connected Routes	641
Configure IP Pools with MPLS Labels	641
Bind DHCP Service for Corporate Servers	641
Bind AAA Group for Corporate Servers	642
DSCP and EXP Bit Mapping	642

CHAPTER 30
Revised Marking for Subscriber Traffic 643

Revised Marking for Subscriber Traffic	643
Feature Description	643
Limitations	643
How It Works	643

Behavior Changes for Different Services	644
Configuring Revised Marking for Subscriber Traffic	644
Configuring Internal Priority	644
Verifying the Configuration	645
Monitoring and Troubleshooting Revised Marking for Subscriber Traffic	645
Internal Priority Show Commands	645
show configuration	645
show service-type { all name service_name }	646

CHAPTER 31

Rejection/Redirection of HA Sessions on Network Failures 647

Overview	647
Configuring HA Session Redirection	648
RADIUS Attributes	651

CHAPTER 32

Policy Forwarding 653

Overview	653
IP Pool-based Next Hop Forwarding	654
Configuring IP Pool-based Next Hop Forwarding	654
Subscriber-based Next Hop Forwarding	654
Configuring Subscriber-based Next Hop Forwarding	654
ACL-based Policy Forwarding	655
Configuring ACL-based Policy Forwarding	655
Applying the ACL to an IP Access Group	655
Applying the ACL to a Destination Context	655
Applying the ACL to an Interface in a Destination Context	656

CHAPTER 33

Proxy-Mobile IP 657

Overview	657
Proxy Mobile IP in 3GPP2 Service	659
Proxy Mobile IP in 3GPP Service	659
Proxy Mobile IP in WiMAX Service	660
How Proxy Mobile IP Works in 3GPP2 Network	660
Scenario 1: AAA server and PDSN/FA Allocate IP Address	661
Scenario 2: HA Allocates IP Address	664
How Proxy Mobile IP Works in 3GPP Network	666

How Proxy Mobile IP Works in WiMAX Network	670
Scenario 1: AAA server and ASN GW/FA Allocate IP Address	671
Scenario 2: HA Allocates IP Address	673
How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication	675
Configuring Proxy Mobile-IP Support	680
Configuring FA Services	680
Verify the FA Service Configuration	681
Configuring Proxy MIP HA Failover	682
Configuring Subscriber Profile RADIUS Attributes	682
Configuring Subscriber Profile RADIUS Attributes	682
RADIUS Attributes Required for Proxy Mobile IP	683
Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN	684
Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF	684
Configuring Default Subscriber Parameters in Home Agent Context	685
Configuring APN Parameters	685

CHAPTER 34

QoS Management	687
Introduction	687
Dynamic QoS Renegotiation	687
How Dynamic QoS Renegotiation Works	688
Initial QoS	688
Service Detection	688
Classification of Application Traffic	689
L4 Packet Inspection	689
L7 Packet Inspection	689
QoS Renegotiation for a Subscriber QoS Profile	689
Network Controlled QoS (NCQoS)	690
How Network Controlled QoS (NCQoS) Works	690
Configuring Dynamic QoS Renegotiation	691
Configuring ACL for Dynamic QoS Renegotiation	692
Configuring Charging Action for Dynamic QoS Renegotiation	692
Configuring Rulebase for Dynamic QoS Renegotiation	693
Configuring APNs for Dynamic QoS Renegotiation	693
Configuring Network Controlled QoS (NCQoS)	694
Configuring Packet Filter for NCQoS	694

Configuring Charging Action for NCQoS	694
Configuring APN for NCQoS	695
Monitoring Dynamic QoS Renegotiation Operation	695
Event IDs Pertaining to Dynamic QoS Renegotiation	696
RADIUS Attributes	696

CHAPTER 35

Remote Address-based RADIUS Accounting 697

Overview	697
License Requirements	697
Configuring Remote Address-based Accounting	698
Verifying the Remote Address Lists	698
Subscriber Attribute Configuration	698
Supported RADIUS Attributes	699
Configuring Local Subscriber Profiles	699

CHAPTER 36

Routing Behind the Mobile Station on an APN 701

Feature Description	701
How It Works	702
Routing Behind the Mobile Station on an APN	702
Configuring Routing Behind the Mobile Station	702
Configuration Overview	703
Creating an APN Profile	703
Enabling Routing Behind the Mobile Station	703
Verifying the Routing Behind the Mobile Station	704
Monitoring and Troubleshooting the Routing Behind the Mobile Station	707
Routing Behind the Mobile Station Show Command(s) and/or Outputs	707
show apn name <apn_name>	707

CHAPTER 37

Rf Interface Support 709

Introduction	709
Offline Charging Architecture	711
Charging Collection Function	712
Charging Trigger Function	712
Dynamic Routing Agent	713
License Requirements	713

Supported Standards	713
Features and Terminology	713
Offline Charging Scenarios	713
Basic Principles	713
Event Based Charging	715
Session Based Charging	715
Diameter Base Protocol	715
Timer Expiry Behavior	717
Rf Interface Failures/Error Conditions	717
DRA/CCF Connection Failure	717
No Reply from CCF	717
Detection of Message Duplication	717
CCF Detected Failure	717
Rf-Gy Synchronization Enhancements	718
Cessation of Rf Records When UE is IDLE	719
QoS Change Scenarios	719
Diameter Rf Duplicate Record Generation	719
Feature Description	720
Configuring Rf Duplicate Record Generation	721
Configuring Secondary AAA Group	721
Configuring Duplication of Rf Records	722
Verifying the Rf Duplicate Record Generation Configuration	722
Monitoring and Troubleshooting the Rf Duplicate Record Generation	723
show diameter aaa-statistics	723
Truncation of Virtual APN for Rf Records	724
Feature Description	724
Configuring Virtual APN Truncation for Rf Records	724
Configuring Gn-APN/VAPN for Rf Accounting	724
Configuring Truncation of Virtual APN	725
Verifying the Virtual APN Truncation Configuration	726
Monitoring and Troubleshooting the Virtual APN Truncation	726
show apn statistics	726
show subscribers ggsn-only full all	726
show subscribers pgw-only full all	727
show subscribers saegw-only full all	727

How it Works	727
Configuring Rf Interface Support	729
Enabling Rf Interface in Active Charging Service	730
Configuring GGSN / P-GW Rf Interface Support	730
Configuring P-CSCF/S-CSCF Rf Interface Support	739
Gathering Statistics	740

CHAPTER 38

Subscriber Overcharging Protection	743
Feature Overview	743
Overcharging Protection - GGSN Configuration	744
GTP-C Private Extension Configuration	745
Verifying Your GGSN Configuration	745
Overcharging Protection - SGSN Configuration	746
Private Extension IE Configuration	747
RANAP Cause Trigger Configuration	747
Verifying the Feature Configuration	747

CHAPTER 39

Traffic Policing and Shaping	749
Overview	749
Traffic Policing	750
Traffic Shaping	750
Traffic Policing Configuration	750
Configuring Subscribers for Traffic Policing	751
Configuring APN for Traffic Policing in 3GPP Networks	752
Traffic Shaping Configuration	753
Configuring Subscribers for Traffic Shaping	754
Configuring APN for Traffic Shaping in 3GPP Networks	754
RADIUS Attributes	756
Traffic Policing for CDMA Subscribers	756
Traffic Policing for UMTS Subscribers	757

CHAPTER 40

Type of Service/Traffic Class Configuration for Predefined Rules	759
Feature Summary and Revision History	759
Feature Description	760
How It Works	760

Limitations	761
Configuring the TOS/Traffic Class for Predefined Rules	762
Enabling or Disabling the ip tos-traffic-class Command	762
Monitoring and Troubleshooting	762
Show Commands	762
show configuration	762
show active-charging packet-filter	763
show configuration verbose	763

APPENDIX A

Engineering Rules	765
APN Engineering Rules	765
DHCP Service Engineering Rules	765
GGSN Engineering Rules	766
GRE Tunnel Interface and VRF Engineering Rules	766
GTP Engineering Rules	766
Interface and Port Engineering Rules	766
Pi Interface Rules	767
FA to HA Rules	767
HA to FA	767
GRE Tunnel Interface Rule	768
Lawful Intercept Engineering Rules	768
MBMS Bearer Service Engineering Rules	768
Service Engineering Rules	768
Subscriber Engineering Rules	769



About this Guide

This preface describes the *Gateway GPRS Support Node Administration Guide*, how it is organized and its document conventions.

Gateway GPRS Support Node (GGSN) is a StarOS application that runs on Cisco® ASR 5500 and virtualized platforms.

- [Conventions Used](#), page xxxvii
- [Supported Documents and Resources](#), page xxxviii

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a screen display	This typeface represents displays that appear on your terminal screen, for example: Login:
Text represented as commands	This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.

Typeface Conventions	Description
Text represented as a command <i>variable</i>	This typeface represents a variable that is part of a command, for example: show card <i>slot_number</i> <i>slot_number</i> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Supported Documents and Resources

Related Common Documentation

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (platform dependant)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependant)
- *Thresholding Configuration Guide*

Related Product Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following product documents are also available and work in conjunction with the GGSN:

- *ADC Administration Guide*
- *CF Administration Guide*
- *ECS Administration Guide*
- *ePDG Administration Guide*

- *HA Administration Guide*
- *HSGW Administration Guide*
- *IPSec Reference*
- *MME Administration Guide*
- *NAT Administration Guide*
- *P-GW Administration Guide*
- *PDSN Administration Guide*
- *PSF Administration Guide*
- *S-GW Administration Guide*
- *SAEGW Administration Guide*
- *SaMOG Administration Guide*
- *SecGW Administration Guide*
- *SGSN Administration Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

<http://www.cisco.com/cisco/web/psa/default.html>

Use the following path selections to access the GGSN documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco GGSN Gateway GPRS Support Node

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of <http://www.cisco.com> for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER

1

GGSN Support in GPRS/UMTS Wireless Data Services

The Cisco systems provides wireless carriers with a flexible solution that functions as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.

This overview provides general information about the GGSN including:

- [Product Description, page 1](#)
- [Product Specification, page 2](#)
- [Network Deployment and Interfaces, page 3](#)
- [Features and Functionality - Base Software, page 8](#)
- [Features and Functionality - Optional Enhanced Feature Software, page 33](#)
- [How GGSN Works, page 50](#)
- [Supported Standards, page 69](#)

Product Description

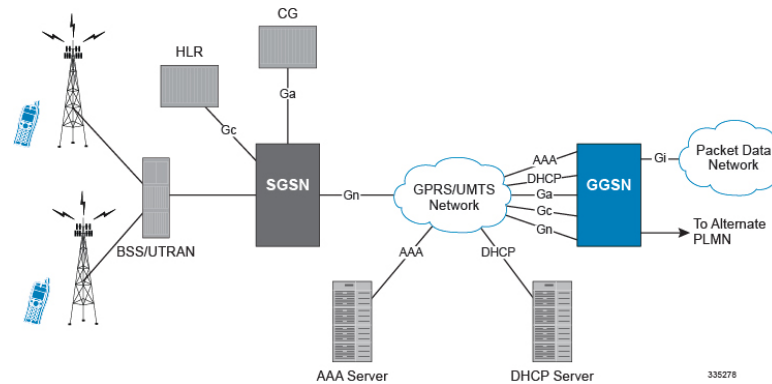
The GGSN works in conjunction with Serving GPRS Support Nodes (SGSNs) within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network
- Provide charging detail records (CDRs) to the charging gateway (CG, also known as the Charging Gateway Function (CGF))
- Route data traffic between the subscriber's Mobile Station (MS) and a Packet Data Networks (PDNs) such as the Internet or an intranet

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

In addition to providing the basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to either function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

Figure 1: Basic GPRS/UMTS Network Topology



In accordance with RFC 2002, the FA is responsible for mobile node registration with, and the tunneling of data traffic to/from the subscriber's home network. The HA is also responsible for tunneling traffic, but also maintains subscriber location information in Mobility Binding Records (MBRs).

Product Specification

This section describes the hardware and software requirements for GGSN service.

This section provides the following information:

- [Licenses, on page 2](#)
- [Qualified Platforms, on page 2](#)
- [Operating System Requirements, on page 3](#)

Licenses

The GGSN is a licensed Cisco product and therefore separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Qualified Platforms

GGSN is a StarOS application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate System Administration Guide and/or contact your Cisco account representative.

Operating System Requirements

The Cisco GGSN is available for ST16 and chassis running StarOS™ Release 7.1 or later.

Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of GGSN in GPRS/UMTS network.

The following information is provided in this section:

- [GGSN in the GPRS/UMTS Data Network, on page 4](#)
- [Supported Interfaces, on page 5](#)

GGSN in the GPRS/UMTS Data Network

The figures shown below display simplified network views of the Cisco GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function; and both GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

Figure 2: Basic GPRS/UMTS Network Topology 1

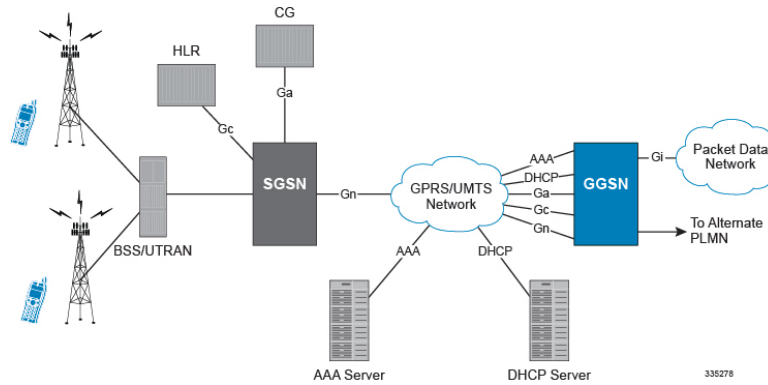


Figure 3: Combined GGSN/FA Deployment for Mobile IP and/or Proxy Mobile IP Support

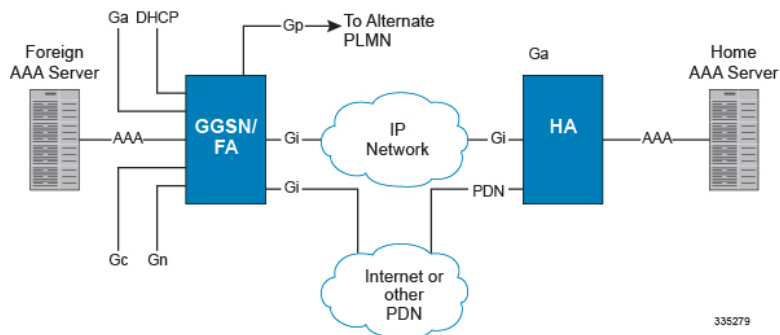
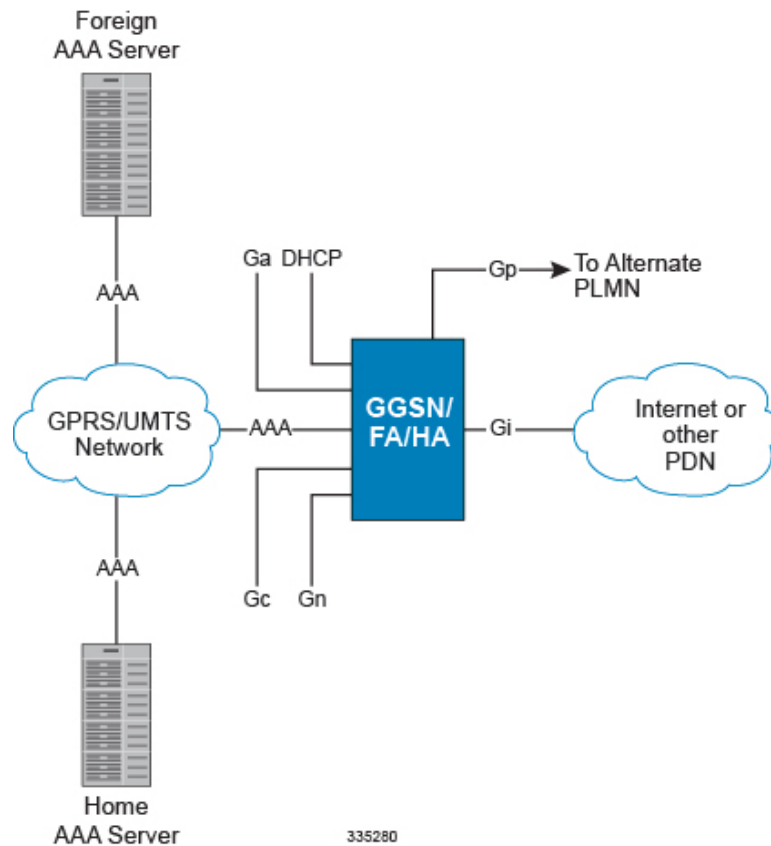


Figure 4: Combined GGSN/FA/HA Deployment for Mobile IP and/or Proxy Mobile IP Support



Supported Interfaces

In support of both mobile and network originated subscriber PDP contexts, the system GGSN provides the following network interfaces:

- **Gn**: This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signaling and the data path for establishing and maintaining subscriber PDP contexts.

The GGSN communicates with SGSNs on the PLMN using GPRS Tunnelling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).



Important

One or more Gn interfaces can be configured per system context.

- **Ga**: This is the interface used by the GGSN to communicate with the Charging Gateway (CG). The charging gateway is responsible for sending GGSN Charging Data Records (G-CDRs) received from the GGSN for each PDP context to the billing system. System supports TCP and UDP as transport layer for this interface.

The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).


Important

One or more Ga interfaces can be configured per system context.

- **Gc:** This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signaling System 7 (SS7).

One Gc interface can be configured per system context.

- **Gi:** This is the interface used by the GGSN to communicate with Packet Data Networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

Inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

For systems configured as a GGSN/FA, this interface is used to communicate with HAs for Mobile IP and Proxy Mobile IP support.

One or more Gi interfaces can be configured per system context. For Mobile IP and Proxy Mobile IP, at least one Gi interface must be configured for each configured FA service. Note that when the system is simultaneously supporting GGSN, FA, and HA services, traffic that would otherwise be routed over the Gi interface is routed inside the chassis.

- **Gp:** This is the interface used by the GGSN to communicate with GPRS Support Nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

One or more Gn/Gp interfaces can be configured per system context.

- **AAA:** This is the interface used by the GGSN to communicate with an authorization, authentication, and accounting (AAA) server on the network. The system GGSN communicates with the AAA server using the Remote Authentication Dial In User Service (RADIUS) protocol.

This is an optional interface that can be used by the GGSN for subscriber PDP context authentication and accounting.

- **DHCP:** This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured as DHCP-Proxy or DHCP Client to provide IP addresses to MS on PDP contexts activation the DHCP server dynamically.

- **Gx:** This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Rule Function (CRF) for the provisioning of charging rules that are based on the dynamic analysis of flows used for an IP Multimedia Subsystem (IMS) session. The system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. It also provides Flow based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage.


Important

The Gx interface is a license-enabled support. For more information on this support, refer *Gx Interface Support* in this guide.

- **Gy:** This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides

an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an "online" or "prepaid" style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.



Important This interface is supported through Enhanced Charging Service. For more information on this support, refer *Enhanced Charging Service Administration Guide*.

- **GRE:** This new protocol interface in GGSN platform adds one additional protocol to support mobile users to connect to their enterprise networks: Generic Routing Encapsulation (GRE). GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).



Important The GRE protocol interface is a license-enabled support. For more information on this support, refer *GRE Protocol Interface Support* in this guide.

- **S6b:** This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.

The S6b interface has the ability to pull SGSN-MCC-MNC from either GTP or AAA-I and send to OCS. When a customer roams into a GSM environment, OCS needs location information for online charging and metering. 3GPP-SGSN-MCC-MNC AVP, and Location Information AVP are defined in Gy and can be used to identify customer location. With this feature, the GGSN collects the value of SGSN-MCC-MNC from the S6b AAA message, so that it can be available to OCS through Gy interface while passing CCR and CCA messages.

From Release 12.2 onwards, the S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers

Release 12.3 onwards, the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the command line interface.

Another enhancement on S6b interface support is the new S6b Retry-and-Continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. This behavior is only applicable to the aaa-custom15 Diameter dictionary.


Important

The S6b interface can still be disabled via the CLI per the existing MOPs in the event of a long-term AAA outage


Important

This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* section of this guide.

- **Rf:** This interface enables offline accounting functions on the GGSN in accordance with the 3GPP Release 8 specifications. The charging data information is recorded at the GGSN for each mobile subscriber UE pertaining to the radio network usage. Due to the transfer of charging information to GGSN, the services being rendered are not affected in real time.


Important

GGSN Software also supports additional interfaces. For more information on additional interfaces, refer *Features and Functionality - Optional Enhanced Feature Software* section.

Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on GGSN service and do not require any additional licenses.


Important

To configure the basic service and functionality on the system for GGSN service, refer configuration examples provide in *GGSN Administration Guide*.

16,000 SGSN Support

With growing roaming agreements, many more GPRS/UMTS networks support certain APNs and therefore the number of SGSNs that could connect to the GGSN increases. This feature increases the number of connected SGSNs thereby allowing a single GGSN service to support a much larger roaming network.

The GGSN service supports a maximum of 16,000 SGSN IP addresses. The chassis limit for bulk statistics collection is also limit to 16,000. No change in configuration is needed to support this feature.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA (RADIUS and Diameter) server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers

are supported per chassis and may be distributed across a maximum of 1,000 APNs. This feature also enables the AAA servers to be distributed across multiple APN within the same context.

**Important**

In 12.3 and earlier releases, refer to the *AAA and GTPP Interface Administration and Reference* for more information on AAA Server Group configuration. In 14.0 and later releases, refer to the *AAA Interface Administration and Reference*.

Access Control List Support

Access Control Lists provide a mechanism for controlling (i.e permitting, denying, redirecting, etc.) packets in and out of the system.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL rules) or filters that control the action taken on packets that match the filter criteria

Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

There are two primary components of an ACL:

- Rule: A single ACL consists of one or more ACL rules. As discussed earlier, the rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

- Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

**Important**

For more information on Access Control List configuration, refer *IP Access Control List* in *System Administration Guide*.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security.

These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ST16 and chassis and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

APN Support

The GGSN's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

Virtual APN Selection feature enables an operator to select Virtual APN based on 4 cc-profile bits and 12 cc-behavior bits or on the basis on complete 16 cc-behavior bits of Charging Characteristics for GGSN, P-GW, and SAEGW nodes, thus utilizing all 16 bits. This functionality is CLI controlled.

Up to 2,048 APNs can be configured in the GGSN. An APN may be configured for any PDP-type and PDP-type for roamers, that is, PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting:** RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication:** Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging:** Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP:** Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, DHCP, DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.
- **Tunneling:** PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- **QoS:** IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all

of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The GGSN's Virtual APN feature allows the carrier to use a single APN to configure differentiated services. The APN that is supplied by the SGSN is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters. The configurable parameters are: the access gateway IP address, bearer access service name, charging characteristics (CC)-profile index, subscribers within an MSISN range, subscriber's mcc/mnc, whether the subscriber is home/visiting/roaming, subscriber's domain name and the radio access (RAT) type including gen, geran, hspa, eutran, utran, and wlan.



Important

For more information on APN configuration, refer *APN Configuration* in *GGSN Service Configuration*.

APN AMBR Support

The APN-AMBR (Aggregated Maximum Bit Rate) limits the aggregate bit rate that can be expected to be provided across all non-GBR PDP contexts/bearers and across all PDN connections of the same APN.

APN-AMBR value is transferred over the Gn and Gx interface.

APN-AMBR is enforced at GGSN to rate limit the traffic across all non-GBR bearers. If APN-AMBR is not supported by SGSN in the network, GGSN derives APN-AMBR AVP to be sent to PCRF in CCR-I from MBR of the initial PDP context received from SGSN. When MBR of any PDP context gets changed by SGSN, GGSN locally authorizes requested MBR unless it is higher than APN-AMBR. In such case, GGSN can either lower the requested MBR or reject it based on local configuration.

Traffic Policing

The Cisco GGSN offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority.

Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

**Important**

For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema.

The following schemas are supported for GGSN service:

- **System:** Provides system-level statistics
- **Card:** Provides card-level statistics
- **Port:** Provides port-level statistics
- **FA:** Provides FA service statistics
- **HA:** Provides HA service statistics
- **IP Pool:** Provides IP pool statistics
- **PPP:** Provides Point-to-Point Protocol statistics
- **GTPC:** Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP:** Provides GPRS Tunneling Protocol - Prime message statistics
- **APN:** Provides Access Point Name statistics
- **RADIUS:** Provides per-RADIUS server statistics
- **ECS:** Provides Enhanced Charging Service Statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates

the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

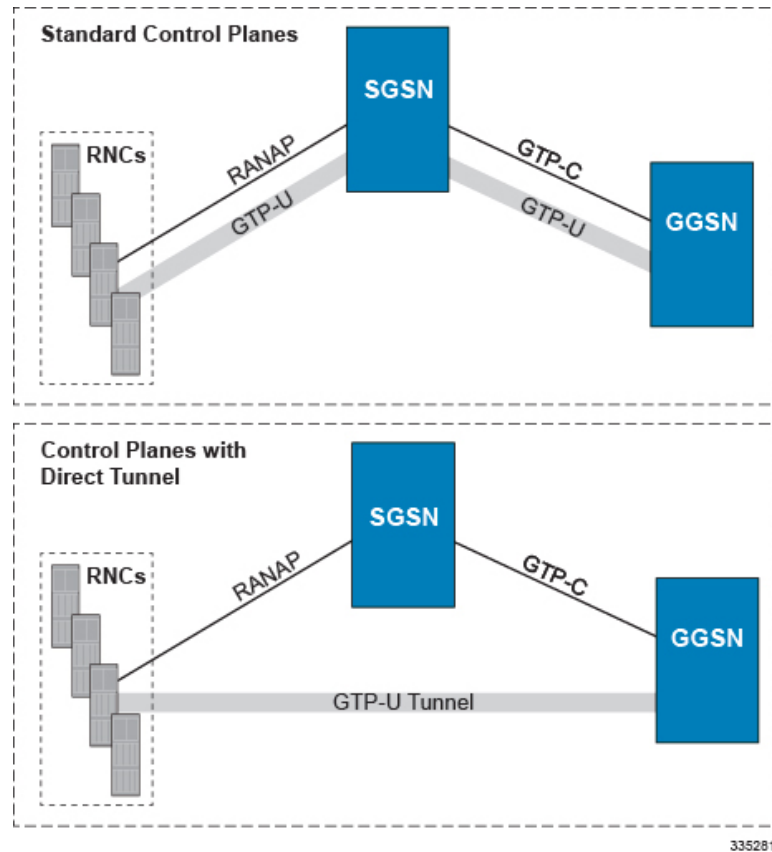
Direct Tunnel Support

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel 'switching' latency from the user plane. An additional advantage of Direct Tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The Direct Tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typically makes the decision to establish Direct Tunnel at PDP Context Activation. A Direct Tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request towards the GGSN).

The following figure illustrates the working of Direct Tunnel between RNC and GGSN.

Figure 5: Direct Tunnel Support in GGSN



A major consequence of deploying Direct Tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced by part of Direct Tunnel deployment. The Cisco GGSN and SGSN offers massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once Direct Tunnel is deployed.

DHCP Support

Dynamic IP address assignment to subscriber IP PDP contexts using the Dynamic Host Control Protocol as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

As described in the PDP Context Support section of this document, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses.

Dynamically assigned IP addresses for subscriber PDP contexts can be assigned through the use of DHCP. The system can be configured to support DHCP using either of the following mechanisms:

- **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.
- **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.



Important

For more information on DHCP service configuration, refer *DHCP Configuration* section in *GGSN Service Configuration* chapter.

DHCPv6 Support

The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of allocating the reusable network addresses and additional configuration functionality automatically.

The DHCPv6 support does not just feature the address allocation, but also fulfills the requirements of Network Layer IP parameters. Apart from these canonical usage modes, DHCPv6's Prefix-Delegation (DHCP-PD) has also been standardized by 3GPP (Rel 10) for "network-behind-ue" scenarios.

GGSN manages IPv6 prefix life-cycle just like it manages IPv4 addresses, thus it is responsible for allocation, renew, and release of these prefixes during the lifetime of a session. IPv6 Prefix is mainly for the UE's session attached to GGSN, where as delegated prefix is for network/devices behind UE. For IPv6 prefixes. GGSN may be obtained from either local-pool, AAA (RADIUS/DIAMETER) or external DHCPv6 servers based on respective configuration. For Delegated IPv6 Prefix allocation, GGSN obtained it from external DHCPv6 servers based on configuration.

Unicast Address Support Feature: The IPv6 prefix delegation for the requested UE is either allocated locally or from an external DHCPv6 server by P-GW, GGSN, SAEGW based on configuration at these nodes. These DHCP messages are sent to the external DHCPv6 server using multicast address as destination address. In networks where there are large number of P-GW servers, but less number of DHCP servers, the DHCPv6 messages with multicast address have to travel through the entire network, increasing load on the network. The Unicast address support feature enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCP service. This feature is CLI controlled and the operator needs to configure a CLI to support for client unicast operation to the DHCP Server.

This DHCPv6 support for GGSN covers below requirement in release 14.0:

- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (Basic DHCPv6)
- RFC 3633, prefix delegation mechanism

**Important**

For more information on DHCPv6 service configuration, refer *DHCPv6 Configuration* section in *GGSN Service Configuration* chapter.

DHCPv6 Prefix Delegation

From release 15.0 onward GGSN supports DHCPv6 Prefix Delegation.

DHCPv6 prefix delegation is required to support deployment models where multiple IPv6 prefixes can be delegated to the UE and which can be further subnetted by the UE and assigned to the links in its internal network. UE will act as a IPv6 router here and will be responsible for just prefix delegation or for prefix delegation along with address assignment and other configuration information. DHCPv6 prefix delegation will allow prefixes to be delegated to the UE independent of bearer establishment and thus without requiring any changes to the mobility signaling protocols.

**Important**

For more information on DHCPv6 prefix delegation configuration, refer *GGSN Service Configuration* chapter.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For different Traffic class, the GGSN supports per-GGSN service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The GGSN supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.

IMS Emergency Session Support

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. These services are provided to normal attached UEs and depending on local regulation, to UEs that are in limited service state. Receiving emergency services in limited service state does not require a subscription. Depending on local regulation and an operator's policy, the SGSN may allow or reject an emergency attach request for UEs in limited service state.

Following four different behaviors of emergency bearer support are included:

- Valid UEs Only: No limited service state UEs are supported in the network. Only normal UEs that have a valid subscription, are authenticated and authorized for PS service in the attached location are allowed. It is not expected that a normal UE would perform an emergency attach. Normal UEs should be attached

to the network and then perform a PDN Connection Request when an IMS emergency session is detected by the UE.

- **Authenticated UEs Only:** These UEs must have a valid IMSI. These UEs are authenticated and may be in limited service state due to being in a location that they are restricted from service. A UE that cannot be authenticated will be rejected.
- **IMSI Required, Authentication Optional:** These UEs must have an IMSI. If authentication fails, the UE is granted access and the unauthenticated IMSI retained in the network for recording purposes. The IMEI is used in the network as the UE identifier. IMEI only UEs will be rejected (e.g., UICCless UEs).
- **All UEs:** Along with authenticated UEs, this includes UEs with an IMSI that cannot be authenticated and UEs with only an IMEI. If an unauthenticated IMSI is provided by the UE, the unauthenticated IMSI is retained in the network for recording purposes. The IMEI is used in the network to identify the UE.

Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the "mobile router." If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session. For more information, see *Routing Behind the Mobile Station on an APN* chapter.

Generic Corporate APN

Any operator may not be aware of the IP address that a corporation may assign to subscribers through AAA or DHCP and the traffic is sent from the GGSN to the corporation over a tunnel, this feature allows the operator to terminate such users.

Normally the GGSN validates the IP address assigned by RADIUS, however this feature removes the need for this, but does assume that the subscriber traffic is forwarded out of the GGSN through a tunnel.

When the IP address is statically assigned, i.e., either MS provided, RADIUS provided or DHCP provided, the IP address validation is not performed if the address policy is set to disable address validation.

ACL and Policy Group Info processing would still be performed.

Additionally, there is support for Virtual APN selection based on RADIUS VSA returned during Authentication.

The existing Virtual APN selection mechanism is being enhanced to select the Virtual APN based on RADIUS VSA returned during authentication.

The selected V-APN may further require AAA authentication (and accounting) with its own servers.

GnGp Handoff Support

In LTE deployments, the smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. Since support

for seamless handover across different access technologies is basic requirement for EPC, PGW needs to support handovers as user equipment (UE) moves across different access technologies.

Cisco's PGW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. Therefore these Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and PGW supports handovers between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the PGW works as an IP anchor for the EPC.



Important Handover is supported for IPv4, IPv6, and IPv4v6 PDN connections

GnGp Handoff in Non-Roaming Scenario

Depending on the existing deployments, PLMN may operate Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access. In such cases, the PGW works as an anchor point for both GERAN/UTRAN and E-UTRAN access. Depending on APN, MME/SGSN select a PGW for each call.

In the home network (non-roaming) when UE firstly attaches to the E-UTRAN, it sets up a PDN connection with some EPS bearers and when the UE moves to Gn/Gp SGSN served GERAN/UTRAN access, handover is initiated from MME to the Gn/Gp SGSN. Gn/Gp SGSN then notifies PGW (with GGSN functionality) about the handoff of EPS bearers. During this handover, each EPS bearer in the PDN connection is converted into a PDP context.

The other way, when the UE first attaches on to Gn/Gp SGSN served GERAN/UTRAN, it sets up PDP contexts, and when the UE moves to E-UTRAN access, handover is initiated from Gn/Gp SGSN to the MME. MME then notifies the PGW (through SGW) about the handoff of PDP contexts to the E-UTRAN access. During this handover, all PDP contexts sharing the same APN and IP address are converted to EPS bearers of same PDN connection. Here one of the PDP context is selected as a Default bearer and rest of the PDP contexts are designated as Dedicated bearers.

GnGp Handoff in Roaming Scenario

In the roaming scenario, the vPLMN (Virtual PLMN) operates Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access and hPLMN (Home PLMN) operates a PGW. Other remaining things work as in non-roaming scenario.



Important For more information on configuration of Gn-Gp Handoff, refer the *Gn-Gp Support Configuration* section of *GGSN Service Configuration Procedures* chapter.

GTPP Support

Support for the GPRS Tunnelling Protocol Prime (GTPP) in accordance with the following standards:

- **3GPP TS 32.015 v3.12.0 (2003-12)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging and billing; GSM call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- **3GPP TS 32.215 v5.9.0 (2005-06)**: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 4)

- **3GPP TS 29.060 v7.9.0 (2008-09)**: Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 6)

The system supports the use of GTPP for PDP context accounting. When the GTPP protocol is used, accounting messages are sent to the Charging Gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. They must always be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level. GGSN charging characteristics consist of a profile index and behavior settings. The profile indexes specify the criteria for closing accounting records based specific criteria.



Important

For more information on GTPP group configuration, refer *GTPP Accounting Configuration* in *GGSN Service Configuration* chapter.

Host Route Advertisement

When subscribers are assigned IP addresses from RADIUS or HLR, yet are allowed to connect to multiple GGSNs through the use of DNS round robin or failover, the IP addresses of the subscribers can be advertised on a per user (host) basis to the Gi network using dynamic routing, thereby providing IP reachability to these users.

IP address pools are configured on the GGSN for many reasons, although one of them is so that the pool subnets can be automatically advertised to the network. These are connected routes and are advertised for all non-tunneling pools.

A configuration **explicit-route-advertise** is provided to the IP pool configuration and when this option is enabled, the subnet(s) of the pool are not added to routing table and routing protocols like OSPF and BGP do not know of these addresses and hence do not advertise the subnet(s).

As calls come up, and addresses from this pool (with the "explicit-route-advertise" flag) are used, the assigned addresses are added to the routing table and these addresses can be advertised by OSPF or BGP through the network or the "redistribute connected" command.

Example

A subscriber connecting to GGSN A with an IP address from a pool P1 will be assigned the IP address and the routing domain will be updated with the host route. When a subscriber connects to GGSN B with an IP

address from the same pool, the subscriber will be assigned the requested IP address and the routing domain will then learn its host route. When the subscriber disconnects, the route is removed from the routing table and the routing domain is updated.

The explicit-route-advertise option can be applied and removed from the pool at any time and the routing tables are updated automatically.

The overlap and resource pool behavior does not change therefore it does not make sense to configure an overlap/resource pool with the "explicit-route-advertise" option.

IP Policy Forwarding

IP Policy Forwarding enables the routing of subscriber data traffic to specific destinations based on configuration. This functionality can be implemented in support of enterprise-specific applications (i.e. routing traffic to specific enterprise domains) or for routing traffic to back-end servers for additional processing.

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.



Important

For more information on IP Policy Forwarding configuration, refer *Policy Forwarding* in this guide.

IP Header Compression - Van Jacobson

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic

- Decreases header overhead
- Reduces packet loss rate over lossy links

The system supports the Van Jacobson (VJ) IP header compression algorithms by default for subscriber traffic.

The VJ header compression is supported as per RFC 1144 (CTCP) header compression standard developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

By default IP header compression using the VJ algorithm is enabled for subscribers. You can also turn off IP header compression for a subscriber.



Important

For more information on IP header compression support, refer *IP Header Compression* in this guide.

IPv6 Support

Native IPv6 support allows for the configuration of interfaces/routes with IPv6 (128 bit) addressing. The increased address space allows for future subscriber growth beyond what is currently possible in IPv4. Native IPv6 support on the Gi interface allows support for packets coming from or destined to a mobile over the Gi interface. IPv6 address assignment is supported from a dynamic or static pool via standard 3GPP attributes. The GGSN can communicate using DIAMETER as the transport protocol for Gx to the AAA. Overlapping address space or resource pools are supported if they are in different VPNs. The VPN subsystem is responsible for the configuration and recovery of IP interfaces and routes. IP resources are grouped into separate routing domains known as contexts. The VPN subsystem creates and maintains each context and the resources associated with them. The existing IPv4 model of interface and route notification will be extended to support IPv6.

This feature allows IPv6 subscribers to connect via the GPRS/UMTS infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

IP version 6 is enhanced version of IP version 4 with following modifications:

- Expanded addressing capabilities with 128 bit for address as compared to 32 bits in IPv4.
- Header format simplification
- Improved support of extensions and options

- Flow labeling capability
- Authentication and Privacy capabilities

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 Interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. The GGSN supports a subset of IPv6 Neighbor Discovery as defined by RFC 2461, including the following:

- The GGSN uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- The GGSN supports configuration of the static IPv6 neighbor (next-hop gateway).
- Link-local addresses will be automatically added to Ethernet type interfaces.
- The GGSN performs Unsolicited Neighbor Advertisement on line card switchover.
- The GGSN will reply to neighbor discovery requests for the node's IPv6 addresses.

ICMPv6 is a protocol for IPv6 networks to allow error reporting and check connectivity via echo messages. The GGSN supports a subset of ICMPv6 as defined by [RFC-4443]. The GGSN replies to the link-local, configured IP address, and the all-hosts IP address.

Native IPv6 Routing allows the forwarding of IPv6 packets between IPv6 Networks. The forwarding lookup is based on a longest prefix match of the destination IPv6 address. The GGSN supports configuration of IPv6 routes to directly attached next hops via an IPv6 Interface.



Important

Native IPv6 is only available on the ASR 5500 or higher platform. In Release 9.0 Native IPv6 is available on the GGSN.

MPLS Forwarding with LDP

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF and therefore it is not a routing protocol.

It generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR) which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

In order to support the increasing number of corporate APNs which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, MPLS backbone automatically negotiates the routes using the labels binded with the IP packets. Cisco GGSN as an LSR learns the default route from the connected provider edge (PE) while the PE populates its routing table with the routes provided by the GGSN.

Overlapping IP Address Pool Support

Overlapping IP Address Pools provides a mechanism for allowing operators to more flexibly support multiple corporate VPN customers with the same private IP address space without the expensive investments in physically separate routers, or expensive configurations using virtual routers.

The system supports two type of overlapping pools: resource and overlap. Resource pools are designed for dynamic assignment only, and use a VPN tunnel, such as a GRE tunnel, to forward and receive the private IP addresses to and from the VPN. Overlapping type pools can be used for both dynamic and static, and use VLANs and a next hop forwarding address to connect to the VPN customer.

To forward downstream traffic to the correct PDP context, the GGSN uses either the GRE tunnel ID, or the VLAN ID to match the packet. When forwarding traffic upstream, the GGSN uses the tunnel and forwarding information in the IP pool configuration, so overlapping pools must be configured in the APN for this feature to be used.

When a PDP context is created, the IP addresses is either assigned from the IP pool, in this case the forwarding rules are also configured into the GGSN at this point. If the address is assigned statically, when the GGSN confirms the IP address from the pool configured in the APN, the forwarding rules are also applied.

The GGSN can scale to as many actual overlapping pools as there are VLAN interfaces per context, and there can be multiple contexts per GGSN, or when using resource then the limit is the number of IP pools. This scalability allows operators, who wish to provide VPN services to customers using the customer's private IP address space, need not be concerned about escalating hardware costs, or complex configurations.



Caution

From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.



Caution

In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.



Important

For more information on IP pool overlapping configuration, refer *VLANs* in *System Administration Guide*.

PDP Context Support

Support for subscriber primary and secondary Packet Data Protocol (PDP) contexts in accordance with the following standards:

- **3GPP TS 23.060 v7.4.0 (2007-9)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- **3GPP TS 29.061 v7.6.0 (2008-09)**: 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN) (Release 4)

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 2,048 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- Type (IPv4, IPv6, IPv4v6, and/or PPP)
- Accounting protocol (GTPP or RADIUS)
- Authentication protocol (CHAP, MSCHAP, PAP, Allow-NOAUTH, IMSI-based, MSISDN-based)
- Charging characteristics (use SGSN-supplied or use configured)
- IP address allocation method (static or dynamic)
- PDP Context timers
- Quality of Service

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

Per APN Configuration to Swap out Gn to Gi APN in CDRs

In order to allow for better correlation of CDRs with the network or application used by the subscriber, a configuration option has been added to the GGSN replace the Gn APN with the Gi (virtual) APN in emitted G-CDRs.

When virtual APNs are used, the operator can specify via EMS or a configuration command that the Gi APN should be used in the "Access Point Name Network Identifier" field of emitted G-CDRs, instead of the Gn APN.

Peer GTP Node Profile Configuration Support

Using this configuration, operator can also control some parameters associated with the configured SGSN; like RAT type. This would be taken from configuration, if CPC request doesn't have RAT type.

From release 15.0 onward, the GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTPC parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules defined.

With support of this functionality the GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTP-C parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be defined.

A new framework of peer-profile and peer-map is introduced for configuration. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers the configuration of GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration.

Peer-map config matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with GGSN service.

With support of this feature the Operators can configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

**Important**

For more information on Peer GTP Node Profile configuration, refer *GGSN Service Configuration* chapter.

Port Insensitive Rule for Enhanced Charging Service

This feature allows a single host or url rule to be applied to two different addresses, one with and one without the port number appended. As adding the port to the address is optional, this means that the number of rules could be halved.

Browser applications can sometimes appended the port number to the host or url when sending the host or URL fields. RFC 2616 for example states that port should be appended but if it is omitted then 80 should be assumed.

When configuring rules to define the content, as the web browser may provide the port number, even if it is the default one of 80 for HTTP, then two of each URL are needed.

Example

```
host = www.w3.org host = www.w3.org:80 or http url = http://213.229.187.118:80/chat/c/wel.w.wml
http url = http://213.229.187.118/chat/c/wel.w.wml
```

This feature provides a means to configure the rule such that the traffic is matched irrespective of the presence of a port number.

A new configurable has been added to the rulebase configuration that will ignore the port numbers embedded in the application headers of HTTP, RTSP, SIP, and WSP protocols.

When this feature is enabled, a single rule, such as "host = www.w3.org" would be matched even if the port number is appended and in this case the host field has the value www.w3.org:80, thereby cutting the number of rules needed by up to a half.

**Important**

For more information on enhanced charging service, refer *Enhanced Charging Service Administration Guide*.

P-CSCF Discovery Support

P-CSCF discovery support ensures the parity between PGW and GGSN implementation for deriving P-CSCF addresses from the various interfaces and local configurations. Following is the order of sequence in which P-CSCF address is to be fetched and returned subsequently:

- P-CSCF info from S6b FQDN based DNS query
- P-CSCF info from Config FQDN based DNS query

- P-CSCF info from IMSA configured table
- P-CSCF info from APN config

P-CSCF Discovery is performed inline with respect to the Call establishment Handoff Procedure and refers to the stored FQDN information. In addition to the above enhancements, following points have also been supported:

- Storing of discovered P-CSCF IPv4 and IPv6 addresses
- SR/ICSR Recovery of P-CSCF IP addresses
- Persistence of FQDN information
- Persistence of P-CSCF values across gngp handoff
- Unification of the P-CSCF Address Element

Quality of Service Support

Provides operator control over the prioritization of different types of traffic.

Quality of Service (QoS) support provides internal processing prioritization based on needs, and DiffServ remarking to allow external devices to perform prioritization.



Important

The feature described here is internal prioritization and DiffServ remarking for external prioritization. For additional QoS capabilities of the GGSN, refer to [Features and Functionality - Optional Enhanced Feature Software](#), on page 33.

External prioritization (i.e., the value to use for the DiffServ marking) is configured for the uplink and downlink directions. In the uplink direction, each APN is configurable for the DiffServ ToS value to use for each of the 3GPP traffic classes. Alternatively, you can configure "pass-through", whereby the ToS value will pass through unchanged.

In the downlink direction, the ToS value of the subscriber packet is not changed, but you can configure what to use for the ToS value of the outer GTP tunnel. The value for ToS is configurable for each of the 3GPP traffic classes. In addition, the connections between the GGSN and one or more SGSNs can be configured as a "GGSN Service", and different values for ToS for the same 3GPP traffic class may be configured for different GGSN Services.

RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000

- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within context contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority:** Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm:** Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create "user defined" RADIUS server groups, as many as 399 (excluding "default" server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the GGSN supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.



Important

In 12.3 and earlier releases, refer to the *AAA and GTPP Interface Administration and Reference* for more information on RADIUS AAA configuration. In 14.0 and later releases, refer to the *AAA Interface Administration and Reference*.

RADIUS VLAN Support

VPN customers often use private address space which can easily overlap with other customers. The subscriber addresses are supported with overlapping pools which can be configured in the same virtual routing context.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature supports following scenarios to be defined in the same context:

- Overlapping RADIUS NAS-IP address for various RADIUS server groups representing different APNs.
- Overlapping RADIUS server IP address for various RADIUS servers groups.

Previously, the above scenarios were supported, albeit only when the overlapping addresses were configured in different contexts. Moreover a static route was required in each context for IP connectivity to the RADIUS server.

The new feature utilizes the same concept as overlapping IP pools such that every overlapping NAS-IP address is giving a unique next-hop address which is then bound to an interface that is bound to a unique VLAN, thereby allowing the configuration to exist within the same context.

RADIUS access requests and accounting messages are forwarded to the next hop defined for that NAS-IP and it is then up to the connected router's forward the messages to the RADIUS server. The next hop address determines the interface and VLAN to use. Traffic from the server is identified as belonging to a certain NAS-IP by the port/VLAN combination.

The number of Radius NAS-IP addresses that can be configured is limited by the number of loopback addresses that can be configured.



Important

For more information on VLAN support, refer *VLANs* in *System Administration Guide*.

Routing Protocol Support

The system's support for various routing protocols and routing mechanism provides an efficient mechanism for ensuring the delivery of subscriber data packets.

GGSN node supports Routing Protocol in different way to provide an efficient mechanism for delivery of subscriber data.

The following routing mechanisms and protocols are supported by the system:

- **Static Routes:** The system supports the configuration of static network routes on a per context basis. Network routes are defined by specifying an IP address and mask for the route, the name of the interface in the current context that the route must use, and a next hop IP address.
- **Open Shortest Path First (OSPF) Protocol:** A link-state routing protocol, OSPF is an Interior Gateway Protocol (IGP) that routes IP packets based solely on the destination IP address found in the IP packet header using the shortest path first. IP packets are routed "as is", meaning they are not encapsulated in any further protocol headers as they transit the network.

Variable length subnetting, areas, and redistribution into and out of OSPF are supported.

OSPF routing is supported in accordance with the following standards:

- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-2328, OSPF Version 2, April 1998
- RFC-3101 OSPF-NSSA Option, January 2003

- **Border Gateway Protocol version 4 (BGP-4):** The system supports a subset of BGP (RFC-1771, A Border Gateway Protocol 4 (BGP-4)), suitable for eBGP support of multi-homing typically used to support geographically redundant mobile gateways, is supported.

EBGP is supported with multi-hop, route filtering, redistribution, and route maps. The network command is support for manual route advertisement or redistribution.

BGP route policy and path selection is supported by the following means:

- Prefix match based on route access list
 - AS path access-list
 - Modification of AS path through path prepend
 - Origin type
 - MED
 - Weight
- **Route Policy:** Routing policies modify and redirect routes to and from the system to satisfy specific routing needs. The following methods are used with or without active routing protocols (i.e. static or dynamic routing) to prescribe routing policy:
 - **Route Access Lists:** The basic building block of a routing policy, route access lists filter routes based upon a specified range of IP addresses.
 - **IP Prefix Lists:** A more advanced element of a routing policy. An IP Prefix list filters routes based upon IP prefixes
 - **AS Path Access Lists:** A basic building block used for Border Gateway Protocol (BGP) routing, these lists filter Autonomous System (AS) paths.
 - **Route Maps:** Route-maps are used for detailed control over the manipulation of routes during route selection or route advertisement by a routing protocol and in route redistribution between routing protocols. This detailed control is achieved using IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System Paths.
 - **Equal Cost Multiple Path:** ECMP allows distribution of traffic across multiple routes that have the same cost to the destination. In this manner, throughput load is distributed across multiple paths, typically to lessen the burden on any one route and provide redundancy.



Important

For more information on IP Routing configuration, refer *Routing in System Administration Guide*.

Subscriber Session Trace Support

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an UMTS environment.

In general, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The UMTS network entities like SGSN and GGSN support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including **Gn**, **Gi**, **Gx**, and **Gmb** interface on GGSN. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at AAA with trace activation via authentication response messages over **Gx** reference interface
- Signaling based activation through signaling from subscriber access terminal



Important

Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the UMTS network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the system. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

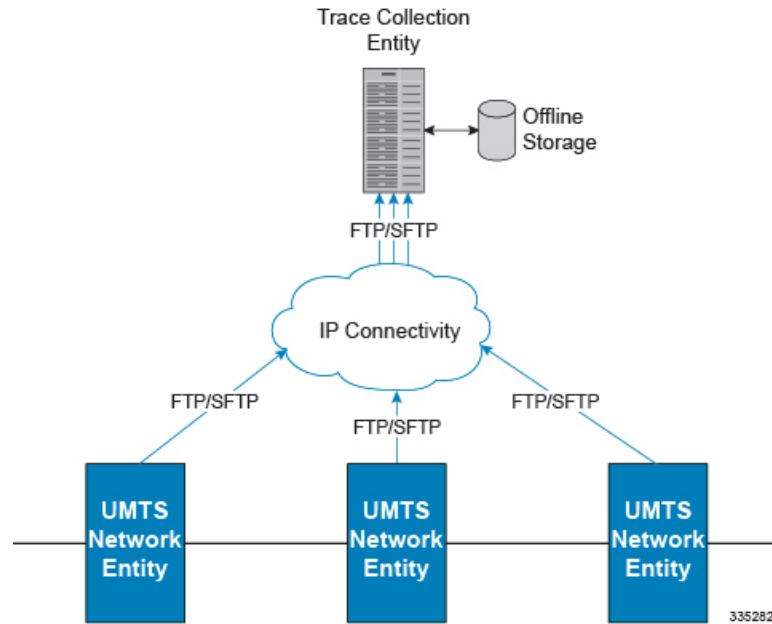


Important

Only Maximum Trace Depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 6: Session Trace Function and Interfaces



All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Support of Charging Characteristics Provided by AAA Server

This feature provides the ability for operators to apply Charging Characteristics (CC) from the AAA server instead of a hard coded local profile during access authentication.

The RADIUS attribute **3GPP-Chrg-Char** can be used to get the charging characteristics from RADIUS in Access-Accept message. Accepting the RADIUS returned charging characteristic profile must be enabled per APN. The CC profile returned by AAA will override any CC provided by the SGSN, the GGSN or per APN configuration. All 16 profile behaviors can be defined explicitly or the default configuration for that profile is used.

Support of all GGSN generated causes for partial G-CDR closure

Provides more detailed eG-CDR and/or G-CDR closure causes as per 3GPP TS 32.298.

System handles the GGSN generated causes for partial closure of CDRs. It supports various type of causes including Radio Access Technology Change, MS Time Zone Change, Cell update, inter-PLMN SGSN change, PLMN id change, QoS, Routing-Area update etc.

Support of ULI/RAI Generation

User Location Information and Routing Area Identity (ULI/RAI) IEs in Create PDP Context Request message identify the Location Area for the UE. This information is passed on the interfaces like Gx, Gy, and Ga. There are circumstances when this information (ULI/RAI) does not come from SGSN, but it has to be relayed on these interfaces.

Release 14.0 onwards, the support has been provided to generate ULI/RAI based on certain CLI configurations on GGSN if it has not come from SGSN.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored value.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING

Logs are supported in both the Alert and the Alarm models.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.

**Important**

For more information on threshold crossing alert configuration, refer *Thresholding Configuration Guide*.

Virtual APN Selection

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the GGSN in conjunction with multiple configurable parameters. Then, the GGSN selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the GGSN. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address

For Virtual APN configuration information, see *Virtual APN Configuration* section in *GGSN Service Configuration Procedures* chapter in this book.

**Important**

For more information, refer to the **virtual-apn preference** command in *APN Configuration Mode Commands* in the *Command Line Interface Reference*.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for GGSN service.

Each of the following features require the purchase of an additional license to implement the functionality with the GGSN service.

Common Gateway Access Support

Common Gateway Access support is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow users to have the same user experience, independent of the access technology available.

In today's scenario an operator must have multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS solution for international roaming. Therefore, operator requires a solution to allow customers

to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

For more information on this product, refer *Common Gateway Access Support* section in GGSN Service Administration Guide.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization:** The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message:** The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.



Important

For more information on dynamic RADIUS extensions support, refer *CoA, RADIUS, And Session Redirection (Hotlining)* in this guide.

GRE Protocol Interface Support

GGSN supports GRE generic tunnel interface support in accordance with RFC-2784, Generic Routing Encapsulation (GRE).

GRE protocol functionality adds one additional protocol on the system to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

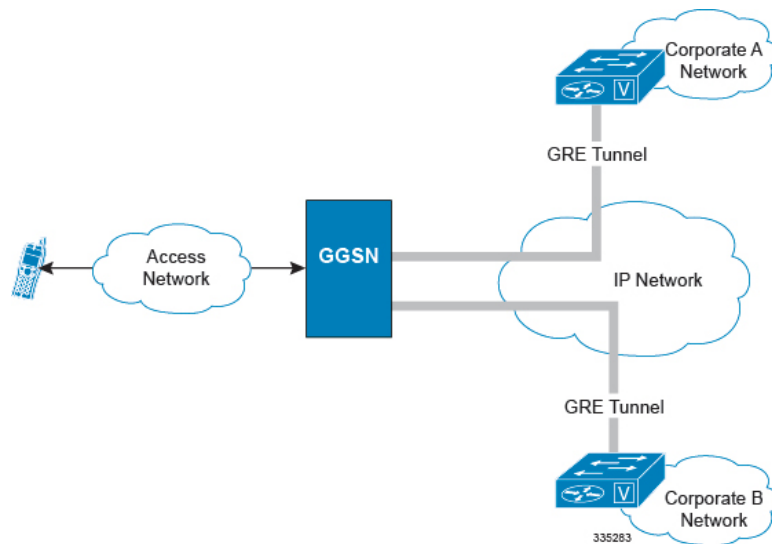
GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSEC.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

The following figure shows a high-level overview of the GRE deployment scenario:

Figure 7: GRE Deployment Scenario



GTP Throttling

From release 15.0 onward, the GGSN supports PDP throttling to help control the rate of incoming/outgoing messages on GGSN. This functionality is used in ensuring GGSN doesn't get overwhelmed by the GTP control plane messages. Also it will help in ensuring the GGSN will not overwhelm the peer GTP-C node with GTP Control plane messages.

This feature covers over-load protection of GGSN nodes and other external nodes with which it communicates. External node overload can happen in a scenario where GGSN generates signaling requests at a higher rate than other nodes can handle. Also if the incoming rate is high at GGSN node, we might flood any of the external nodes. Hence throttling of both incoming and outgoing control messages is required.

**Important**

GTP throttling will be done only for session level control messages. Path management messages will not be rate limited.

**Important**

For more information on GTP throttling configuration, refer *GGSN Service Configuration* chapter.

Bypass Rate Limit Function

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature.

This enhancement requires no additional license. Existing licenses for the GTP-Throttling Feature (RLF License) and the VoLTE Prioritized Handling feature have been applied and used as follows:

- **RLF License:** The GTP-Throttling feature license has been enhanced to accommodate the message-types based RLF throttling bypass.
- **VoLTE Prioritized Handling Feature License:** This license has been enhanced to accommodate the emergency call, priority call, and apn-names based RLF throttling bypass.

The GTP Throttling feature helps control the rate of incoming/outgoing messages on GGSN. It prevents the message flood from P-GW towards S-GW and MME. Currently, following outgoing messages are throttled by GGSN using the RLF framework:

- Create Bearer Request (CBR)
- Delete Bearer Request (DBR)
- Update Bearer Request (UBR)
- NRUPC
- IPCA
- NRDPC

Once throttling is enabled for outgoing messages, all outgoing messages are throttled except the Create Bearer Request (CBR) message, which is piggybacked with Create Session Response message.

This feature has been enhanced to control the bypassing of some messages being throttled.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.

**Important**

For more information on these commands, refer to the *CLI Reference Guide*.

Gx Interface Support

Gx interface support on the system enables the wireless operator to:

- Implement differentiated service profiles for different subscribers
- Intelligently charge the services accessed depending on the service type and parameters

This interface is particularly suited to control and charge multimedia applications and IMS services. This interface support is compliant to following standards:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.210 V6.2.0 (2005-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Charging rule provisioning over Gx interface; (Release 6)
- 3GPP TS 29.212 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol
- RFC 4006, Diameter Credit-Control Application

In addition to the above RFCs and standards IMS authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

The goal of the Gx interface is to provide network based QoS control as well as dynamic charging rules on a per bearer basis. The Gx interface is in particular needed to control and charge multimedia applications.

QoS Parameter ARP Setting via Gx Interface: GGSN controls the assignment of different radio interface QoS priorities (gold/silver/bronze) via the PCRF Gx interface during PDP context setup (CCR/CCA-I). This is performed using the Allocation Retention Priority (ARP) parameter (AVP code 1034) as specified in 3GPP TS 29.212, with values = 0-3; ARP values from the PCRF other than 0-3 are ignored. During PDP context setup the PCRF returns the ARP value in CCA-I and this ARP is then assigned/negotiated with the SGSN and RNC.

The Gx interface is located between the GGSN and the E-PDF / PCRF. It is a Diameter- based interface and provides the functions provided earlier by the Gx and Go interfaces:

- QoS control based on either a token-based or token-less mechanism. In the token-based mechanism, the E-PDF or PCRF dynamically assign network resources to the different bearers used by the subscriber. These resource assignments are transmitted in Tokens carried over the Gx interface. The authorization tokens are allocated by the network (E-PDF/PCRF), hence the network is in full control of the mechanism since it only authorizes resources. The token-less mechanism is for further study.
- Dynamic rules for Flexible Bearer Charging. These dynamic charging rules are carried in the resource assignment tokens and provide 5-tuple type charging rules that enables to implement a specific charging

policy for each subscriber bearer. These charging rules will be applied by the FBC function of the GGSN, and produce the appropriate eG-CDRs or the appropriate messages on the Gy interface to the OCS.



Important

For more information on Gx interface support, refer *Gx Interface Support* in this guide.

Inter-Chassis Session Recovery

The ST16 and chassis provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though chassis provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the GGSN Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Inter-chassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange **Hello** messages between the primary and backup chassis and must be maintained for proper system operation.

Interchassis Session Recovery uses following for failur handling and communication:

- **Interchassis Communication:**

Chassis configured to support Interchassis Session Recovery communicate using periodic **Hello** messages. These messages are sent by each chassis to notify the peer of its current state. The **Hello** message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a **Hello** message to be received from the chassis' peer. If the standby chassis does not receive a **Hello** message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

- router identifier

- chassis priority
- SPI MAC address

- **Checkpoint Message:**

Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.


Important

For more information on inter-chassis session recovery support, refer *Interchassis Session Recovery in System Administration Guide*.

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

GGSN supports IPSec features that you may wish to include in your configuration. Refer to the StarOS IP Security (IPSec) Reference for additional information.

IPNE Service Support

The GGSN supports the IP Network Enabler (IPNE) service. IPNE is a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services. For detailed information on IPNE, refer to the IP Network Enabler appendix in this guide.

IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
- IPv6 Interface ID from the RADIUS Server



Important

For more information on IPv6 Prefix Delegation, refer *IPv6 Prefix Delegation from the RADIUS Server and the Local Pool* chapter.

L2TP LAC Support

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the GGSN and the corporation, an L2TP tunnel must be setup in the GGSN running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the GGSN and benefits from dynamic resource allocation and distributed message and data processing. This design allows the LAC service to support over 4000 setups per second or a maximum of over 3G of throughput. There can be a maximum up to 65535 sessions in a single tunnel and as many as 500,000 L2TP sessions using 32,000 tunnels per system.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware or software issues. Tunnel state is preserved by copying the information across processor cards.



Important

For more information on this feature support, refer *L2TP Access Concentrator* in this guide.

L2TP LNS Support

The system configured as a Layer 2 Tunneling Protocol Network Server (LNS) supports the termination secure Virtual Private Network (VPN) tunnels between from L2TP Access Concentrators (LACs).

The LNS service takes advantage of the high performance PPP processing already supported in the system design and is a natural evolution from the LAC. The LNS can be used as a standalone, or running alongside a GGSN service in the same platform, terminating L2TP services in a cost effective and seamless manner.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. There can be a maximum of up to 65535 sessions in a single tunnel and up to 500,000 sessions per LNS.

The LNS architecture is similar to the GGSN and utilizes the concept of a de-multiplexer to intelligently assign new L2TP sessions across the available software and hardware resources on the platform without operator intervention.


Important

For more information on this feature support, refer *L2TP Network Server* in this guide.

Lawful Intercept

The system supports the Lawful Interception (LI) of subscriber session information. This functionality provides Telecommunication Service Providers (TSPs) with a mechanism to assist Law Enforcement Agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

The following standards were referenced for the system's LI implementation:

- TR-45 Lawfully Authorized Electronic Surveillance TIA/EIA J-STD-025 PN4465 RV 1.7
- 3GPP TS 33.106 V6.1.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 6)
- 3GPP TS 33.107 V6.2.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 6)
- 3GPP TS 33.108 V9.0.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 9)
- Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ), Version 4.0

LEAs provide one or more TSPs with court orders or warrants requesting the monitoring of a particular target. The target is identified by information such as their mobile station Integrated Services Digital Network (MSISDN) number, or their International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the system, functioning as either a GGSN or HA, serves as an Access Function (AF) and performs monitoring for both new PDP contexts or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface. Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

Lawful intercept supports TCP transport on node interfaces along with support for IPv6 address link between chassis and LI server.

On the system with StarOS version 9.0 or later, this feature enhanced to allow 20,000 LI targets to be provisioned as well as monitored.


Caution

This capacity improvement impacts performance over various network scenario and in order to reach the full target of 20000 LI targets, it is required that the used platform have at least 12 active packet processing cards installed.

**Important**

For more information on this feature support, refer *Lawful Intercept Configuration Guide*.

Mobile IP Home and Foreign Agents

Consolidation of GGSN, HA and/or FA services on the same platform eliminates CapEx and OpEx requirements for separate network elements and devices under management. Service integration also enables seamless mobility and inter-technology roaming between 1xEV-DO and UMTS/W-CDMA/GPRS/EDGE radio access networks. This shared configuration also enables common address pools to be applied across all service types. In addition, this combination of collapsed services does not create dependencies for Mobile IP client software on the user access device and consequently does not introduce additional requirements for Mobile IP signaling in the 3GPP radio access network.

This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

The system is capable of supporting both GGSN and Mobile IP functions on a single chassis. For Mobile IP applications, the system can be configured to provide the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA).

HA and FA components are defined by RFC 2002 in support of Mobile IP. Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

When configured to support HA functionality, the system is capable of supporting following enhanced features:

- **Mobile IP HA Session Rejection/Redirection:** Enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner. This feature provides the benefit of reducing OpEx through increased operational efficiency and limiting of system downtime.
- **Mobile IP Registration Revocation:** Registration Revocation is a general mechanism whereby the HA providing Mobile IP or Proxy Mobile IP functionality to a mobile node can notify the GGSN/FA of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HA by any of the following:
 - Administrative clearing of calls
 - Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)
 - Session Idle timer expiry (when configured to send Revocation)
 - Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested)

**Important**

For more information on Mobile IP HA service and FA service configuration, refer *HA Administration Guide* and *GGSN Administration Guide* respectively

Mobile IP NAT Traversal

This functionality enables converged WiFi-cellular data deployments in which the system is used to concentrate and switch traffic between WiFi hotspots. UDP/IP tunneling enables NAT firewalls in WLAN hotspots to maintain state information for address translation between NATed public address/UDP ports and addresses that are privately assigned for the mobile access device by a local DHCP server.

The Mobile IP protocol does not easily accommodate subscriber mobile nodes that are located behind WLAN or WAN-based NAT devices because it assumes that the addresses of mobile nodes or FA's are globally routable prefixes. However, the mobile node's co-located care of address (CCoA/CoA) is a private address. This presents a problem when remote hosts try to reach the mobile node via the public advertised addresses. The system provides a solution that utilizes UDP tunneling subject to subscriber reservation requests. In this application, the HA uses IP UDP tunneling to reach the mobile subscriber and includes the same private address that was provided in original reservation request in the encapsulated IP payload packet header.

**Important**

For more information on this feature, refer *MIP NAT Traversal* in *System Administration Guide*.

NEMO Service Support

Use of NEMO requires a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The GGSN provides the configuration support to enable or disable the Network Mobility (NEMO) service on chassis.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the GGSN platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

**Important**

For more information on NEMO support, refer to the *Network Mobility (NEMO)* chapter in this guide.

Multimedia Broadcast Multicast Services Support

Multimedia services are taking on an ever-increasing role in the wireless carriers' plans for an application centric service model. As such, any next generation GGSN platform must be capable of supporting the requirements of multimedia service delivery, including:

- Higher bandwidth requirements of streaming audio and video delivery
- Efficient broadcast and multicast mechanisms, to conserve resources in the RAN

MBMS represents the evolutionary approach to multicast and broadcast service delivery. MBMS uses spectrum resources much more efficiently than Multicast-over-Unicast by optimizing packet replication across all critical components in the bearer path. Thus, services requiring largely uni-directional multicast flows towards the UE are particularly well suited to the MBMS approach. These would include news, event streaming, suitably encoded/compressed cable/radio programs, video-on-demand, multi-chat / group-push-to-talk/video-conferencing sessions with unicast uplink and multicast downlink connections, and other applications.

For MBMS functionality, the system supports the Gmb interface, which is used signal to the BM-SC


Important

For more information on this feature, refer *Multicast Broadcast Service* in this guide.

Overcharging Protection on Loss of Coverage

This solution provides the ability to configure mobile carriers to maximize their network solutions and balancing the requirements to accurately bill their customer.

Considering a scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN is unaware of such loss of connectivity as SGSN does not perform the Update PDP Context procedure to set QoS to 0kbps (this is done when traffic class is either Streaming or Conversational only). The GGSN continues to forward the downlink packets to SGSN. In the loss of radio coverage, the SGSN will do paging request and find out that the mobile is not responding; SGSN will then drops the packets. In such cases, the G-CDR will have increased counts but S-CDR will not. This means that when operators charge the subscribers based on G-CDR the subscribers may be overcharged. This feature is implemented to avoid the overcharging in such cases.

This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.


Important

For more information on this feature, refer *Subscriber Overcharging Protection* in this guide.

Proxy Mobile IP

Mobility for subscriber sessions is provided through the Mobile IP protocol as defined in RFCs 2002-2005. However, some older Mobile Nodes (MNs) do not support the Mobile IP protocol. The Proxy Mobile IP feature provides a mobility solution for these MNs.

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, an AAA server, or on a static-basis. The address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.



Important

For more information on this feature, refer *Proxy Mobile IP* in this guide.

Session Persistence



Important

Other licenses (i.e. IP Security and L2TP) may be additionally required depending on your network deployment and implementation.

Provides seamless mobility to mobile subscribers as they roam between WLAN and 3G cellular access networks. This type of inter-technology roaming is ordinarily not possible as wireline access networks do not include SGSNs to permit inter-SSGN call hand-offs with cellular access networks.

The Cisco Session Persistence Solution maintains consistent user identities and application transparency for your mobile subscribers as they roam across bearer access networks. This is accomplished through the integration of Home Agent (HA) and GGSN functionality on the wireless access gateway in the packet network and the use of standards-based protocols such as Mobile IP and Mobile IP NAT Traversal. The solution also includes Session Persistence client software that runs on dual-mode WiFi/GPRS/EDGE and/or UMTS/W-CDMA access devices including cellular phones and laptop computers with wireless data cards.

The Session Persistence client is designed to permit Mobile IP tunneling over the applicable underlying network including cellular access connections and cable or XDSL broadband access networks. When the user is attached to a WiFi access network, the Session Persistence client utilizes a Mobile IP Co-located Care of Address Foreign Agent Service (CCoA FA) and establishes a MIP tunnel to the HA service in the platform. This scenario is completely transparent to the GGSN service that operates in the same system. The Mobile IP protocol requires a publicly addressable FA service; however, this is a problem when the mobile subscriber is located behind a NAT firewall. In this case, the NAT firewall has no way of maintaining state to associate the public NATed address with the private address assigned to the user by local DHCP server. Mobile IP NAT Traversal solves this problem by establishing a UDP/IP tunnel between the subscriber access device and Home Agent. The NAT firewall uses the UDP port address to build state for the subscriber session. During this Mobile IP transaction, the HA establishes a mobility binding record for the subscriber session.

When the subscriber roams to a 3GPP cellular access network, it uses the IP address from normal PDP IP context establishment as its new Mobile IP Care of Address to refresh the mobility binding record at the Home Agent. For reduced latency between access hand-offs, it is also possible to utilize a permanent 'always-on' PDP IP context with the IP address maintained in the MIP session persistence client. In this scenario, the mobile access device only needs to re-establish the dormant RAB wireless connection with the 3GPP access network prior to transmitting a new Mobile IP registration.

The system also enables network-provisioned VPNs for Session Persistence applications by permitting use of overlapping address pools on the HA and using various tunneling protocols including IPSEC, Layer 2 Tunneling Protocol (L2TP) and Ethernet IEEE 802.1Q VLANs for separation of subscriber traffic. This

application may be further augmented by additional features such as 800 RADIUS Server Groups to permit use of enterprise controlled AAA servers and custom dictionaries.

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of "standby mode" session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby packet processing card.

There are following modes of Session Recovery:

- **Task recovery mode:** Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby packet processing card. In this mode, recovery is performed by using the mirrored "standby-mode" session manager task(s) running on active packet processing cards. The "standby-mode" task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode:** Used when a packet processing card hardware failure occurs, or when a packet processing card migration failure happens. In this mode, the standby packet processing card is made active and the "standby-mode" session manager and AAA manager tasks on the newly activated packet processing card perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processing cards to ensure task recovery.



Important

For more information on this feature, refer *Session Recovery in System Administration Guide*.

Traffic Policing and Rate Limiting

Allows the operator to proportion the network and support Service-level Agreements (SLAs) for customers.

The Traffic-Policing feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular 3GPP traffic class. Values for traffic classes are defined in 3GPP TS 23.107 and are negotiated with the SGSN during PDP context activation using the values configured for the APN on the GGSN. Configuration and enforcement is done independently on the downlink and the uplink directions for

each of the 3GPP traffic classes. Configuration is on a per-APN basis, but may be overridden for individual subscribers or subscriber tiers during RADIUS authentication/authorization.

A Token Bucket Algorithm (a modified trTCM, as specified in RFC2698) is used to implement the Traffic-Policing feature. The algorithm measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets may be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that packets may be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that may be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the configured burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size. After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- There are not enough tokens in the PBS bucket to allow a packet to pass, then the packet is considered to be in violation and is marked "red" and the violation counter is incremented by one.
- There are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS "bucket", then the packet is considered to be in excess and is marked "yellow", the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- There are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked "green" and the CBS and PBS buckets are decremented by the packet size.

The APN on the GGSN can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS octet is set to "0", thus downgrading it to Best Effort, prior to passing the packet.
- **Buffer the Packet:** The packet stored in buffer memory and transmitted to subscriber once traffic flow comes in allowed bandwidth.

Different actions may be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.



Important

For more information on this feature, refer *Traffic Policing* in this guide.

User Location Change Reporting Support

The user information change reporting is enabled on GGSN via PCRF using GPRS specific event triggers and GPRS specific credit re-authorization triggers. The user information to be reported include Location Change Reporting (ULI) and Closed Subscriber Group Information Change reporting (UCI)

For Location change reporting for a subscriber session requested by GGSN, the SGSN includes the User Location Information (ULI) if the MS is located in a RAT Type of GERAN, UTRAN or GAN. It also includes the CGI, SAI or RAI depending on whether the MS is in a cell, a service or a routing area respectively. The SGSN may optionally include the User Location Information for other RAT Types.

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG info change reporting for a subscriber session requested by GGSN, the SGSN includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

Release 20.0 and later, support has been added to process and handle a MS Info Change notification received with valid information to identify a PDN (non-zero TEID and/or IMSI+NSAPI) and with appropriate ULI and/or UCI information. In case of collision between MS-Info-change message and NRUPC, GGSN will process MS-info-change request first and send out its MS-info-change response. Then the NRUPC will be retried again.



Important CSG reporting is not yet supported on GGSN, P-GW, or SAEGW.

Limitations

Following are the limitations of this feature:

- UCI trigger from PCRF is not supported.
- The MS Info Change reporting action trigger will not be recovered if trigger if:
 - trigger is changed
 - MS reporting action has not gone in CPC/UPC/NRUPC
 - session manager (SM) recovery happens
- The MS Change info message is not supported if it comes on UE level.

3GPP ULI Reporting Support Enhanced

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

Feature Change

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Action towards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

Behavior Change

Previous of Change Reporting Action: Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

Behavior of MS Info Change Reporting Action: Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

Limitations

- 1 In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
- 2 In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.

How GGSN Works

This section provides information on the function of the GGSN in a GPRS/UMTS network and presents call procedure flows for different stages of session setup.

The following topics and procedure flows are included:

- [PDP Context Processing](#)
- [Dynamic IP Address Assignment](#), on page 51
- [Subscriber Session Call Flows](#), on page 52

PDP Context Processing

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 2,048 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- **Type:** The system supports IPv4, IPv6, IPv4v6, and PPP PDP contexts. For IPv6 PDP configuration to work, at least one IPv6 interface needs to be configured in the destination context.
- **Accounting protocol:** Support is provided for using either the GTPP or Remote Authentication Dial-In User Service (RADIUS) protocols. In addition, an option is provided to disable accounting if desired.
- **Authentication protocol:** Support is provided for using any of the following:
 - Challenge Handshake Authentication Protocol (CHAP)
 - Microsoft CHAP (MSCHAP)
 - Password Authentication Protocol (PAP)
 - IMSI-based authentication

- MSISDN-based authentication

In addition, an option is provided to disable authentication if desired.

- **Charging characteristics:** Each APN template can be configured to either accept the charging characteristics it receives from the SGSN for a PDP context or use its own characteristics.
- **IP address allocation method:** IP addresses for PDP contexts can be assigned using one of the following methods:
 - **Statically:** The APN template can be configured to provide support for MS-requested static IP addresses. Additionally, a static address can be configured in a subscriber's profile on an authentication server and allocated upon successful authentication.
 - **Dynamically:** The APN template can be configured to dynamically assign an IP address from locally configured address pools or via a Dynamic Host Control Protocol (DHCP) server. Additional information on dynamic address assignment can be found in the *Dynamic IP Address Assignment* section that follows.



Important

Static IP addresses configured in subscriber profiles must also be part of a static IP address pool configured locally on the system.

- **Selection mode:** The MS's right to access the APN can be either verified or unverified. For verified access, the SGSN specifies the APN that should be used. For unverified access, the APN can be specified by either the SGSN or the MS.
- **Timeout:** Absolute and idle session timeout values specify the amount of time that an MS can remain connected.
- **Mobile IP configuration:** Mobile IP requirements, HA address, and other related parameters are configured in the APN template.
- **Proxy Mobile IP support:** Mobile IP support can be enabled for all subscribers facilitated by the APN. Alternatively, it can be enabled for individual subscribers via parameters in their RADIUS or local-user profiles.
- **Quality of Service:** Parameters pertaining to QoS feature support such as for Dynamic Renegotiation, Traffic Policing, and DSCP traffic class.

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

Dynamic IP Address Assignment

IP addresses for PDP contexts can either be static—an IP address is permanently assigned to the MS—or dynamic—an IP address is temporarily assigned to the MS for the duration of the PDP context.

As previously described in the *PDP Context Processing* section of this chapter, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. If dynamic addressing is supported, the following methods can be implemented:

- **Local pools:** The system supports the configuration of public or private IP address pools. Addresses can be allocated from these pools as follows:
 - **Public pools:** Provided that dynamic assignment is supported, a parameter in the APN configuration mode specifies the name of the local public address pool to use for PDP contexts facilitated by the APN.
 - **Private pools:** Provided that dynamic assignment is supported, the name of the local private pool can be specified in the subscriber's profile. The receipt of a valid private pool name will override the APN's use of addresses from public pools.
- **Dynamic Host Control Protocol (DHCP):** The system can be configured to use DHCP PDP context address assignment using either of the following mechanisms:
 - **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.
 - **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

In addition to the above methods, IP addresses for subscriber Mobile IP sessions are also dynamically assigned by the subscriber's home network upon registration. The GGSN/FA, in turn, provide the assigned address to the mobile station.

Subscriber Session Call Flows

This section provides information on how GPRS/UMTS subscriber data sessions are processed by the system GGSN. The following data session scenarios are provided:

- **Transparent IP:** The subscriber is provided basic access to a PDN without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDU) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscriber's PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.

Limitations:

- Secondary PDP context creation for GGSN PDP type PPP session is not supported.
- PDP type PPP for GnGp GGSN is not supported.
- Routing Behind Mobile Station functionality for GGSN PDP-type PPP is not supported.

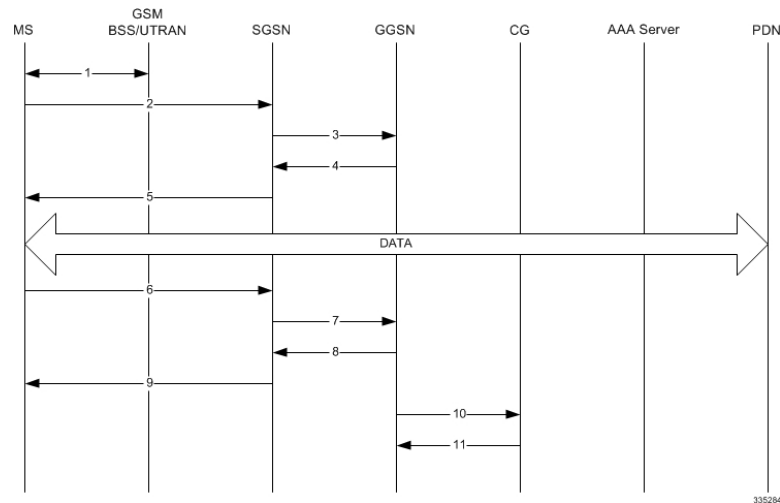
- Inter-Chassis session recovery of GGSN PDP-type PPP sessions is not supported.
 - Multi-PDN with PDP-type PPP is not supported.
 - Inter-RAT handovers with PDP-type PPP is not supported.
 - L2TP with PDP-type PPP is not supported in this release.
 - Lawful Interception with PDP-type PPP is not supported.
 - Static IP address allocation with PDP-type PPP is not supported.
 - IPv6 address allocation with PDP-type PPP is not supported.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
 - **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using IP-in-IP.
 - **Mobile IP:** Subscriber traffic is routed to their home network via a tunnel between the GGSN/FA and an HA. The subscriber's IP PDP context is assigned an IP address from the HA.
 - **Proxy Mobile IP:** Provides a mobility solution for subscribers whose Mobile Nodes (MNs) do not support the Mobile IP protocol. The GGSN/FA proxy the Mobile IP tunnel with the HA on behalf of the MS. The subscriber receives an IP address from their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.
 - **IPv6 Stateless Address Auto Configuration:** The mobile station may select any value for the interface identifier portion of the address. The only exception is the interface identifier for the link-local address used by the mobile station. This interface identifier is assigned by the GGSN to avoid any conflict between the mobile station link-local address and the GGSN address. The mobile station uses the interface ID assigned by the GGSN during stateless address auto-configuration procedure (e.g., during the initial router advertisement messages). Once this is over, the mobile can select any interface ID for further communication as long as it does not conflict with the GGSN's interface ID (that the mobile would learn through router advertisement messages from the GGSN).

Additionally, information about the process used by the system to dynamically assign IP addresses to the MS is provided in following sections.

Transparent Session IP Call Flow

The following figure and the text that follows describe the call flow for a successful transparent data session.

Figure 8: Transparent IP Session Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 3 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
- 4 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this guide.

The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

- 5 The SGSN returns an Activate PDP Context Accept response to the MS.

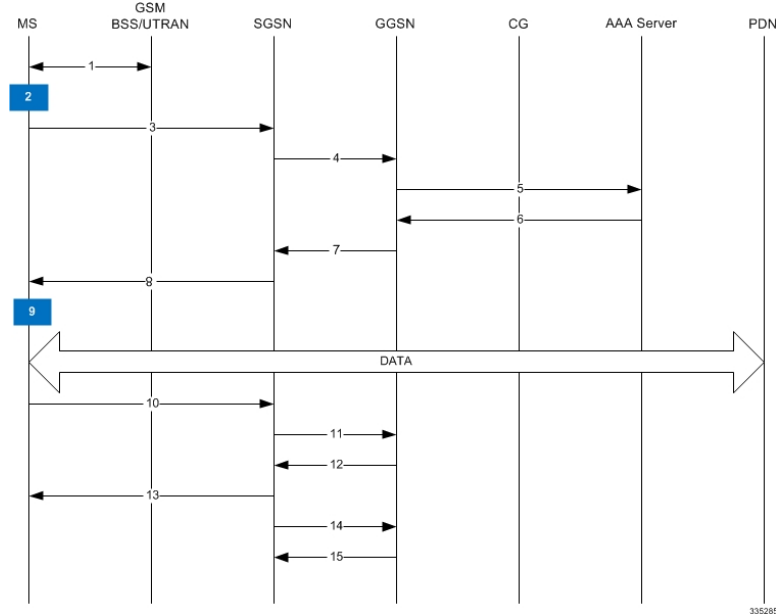
The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.

- 6 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 7 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
- 8 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
- 9 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 10 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 11 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Non-Transparent IP Session Call Flow

The following figure and the text that follows describe the call flow for a successful non-transparent data session.

Figure 9: Non-Transparent IP Session Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication

Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

- 3 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 4 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).
- 5 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, how an IP address should be assigned if using dynamic allocation, and how to route the session.

If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.
- 6 If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
- 7 The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
- 8 The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
- 9 The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

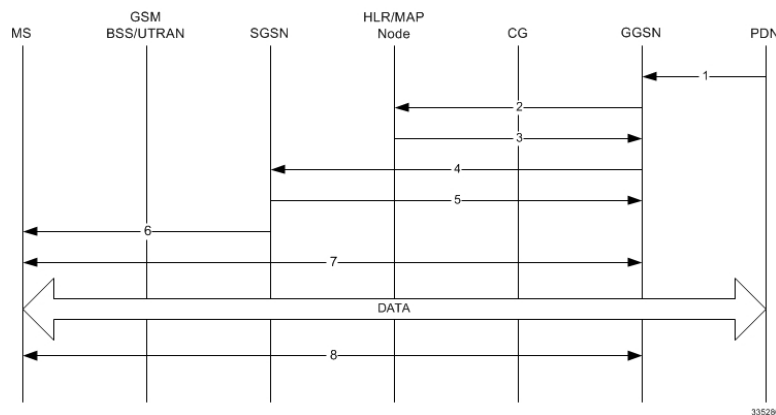
The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
- 10 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 11 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
- 12 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.

- 13 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 14 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 15 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Network-Initiated Session Call Flow

The following figure and the text that follows describe the call flow for a successful network-initiated data session.

Figure 10: Network-initiated Session Call Flow



- 1 An IP Packet Data Unit (PDU) is received by the GGSN from the PDN. The GGSN determines if it is configured to support network-initiated sessions. If not, it will discard the packet. If so, it will begin the Network-Requested PDP Context Activation procedure.
- 2 The GGSN may issue a Send Routing Information for GPRS request to the HLR to determine if the MS is reachable. The message includes the MS's International Mobile Subscriber Identity (IMSI).
- 3 If the MS is reachable, the HLR returns a Send Routing Information for GPRS Ack containing the address of the SGSN currently associated with the MS's IMSI.
- 4 The GGSN sends a PDU Notification Request message to the SGSN address supplied by the HLR. This message contains the IMSI, PDP Type, PDP Address, and APN associated with the session.
- 5 The SGSN sends a PDU Notification Response to the GGSN indicating that it will attempt to page the MS requesting that it activate the PDP address indicated in the GGSN's request.
- 6 The SGSN sends a Request PDP Context Activation message to the MS containing the information supplied by the GGSN.
- 7 The MS begins the PDP Context Activation procedure as described in *step 2* through *step 5* of the *Transparent Session IP Call Flow* section of this chapter.

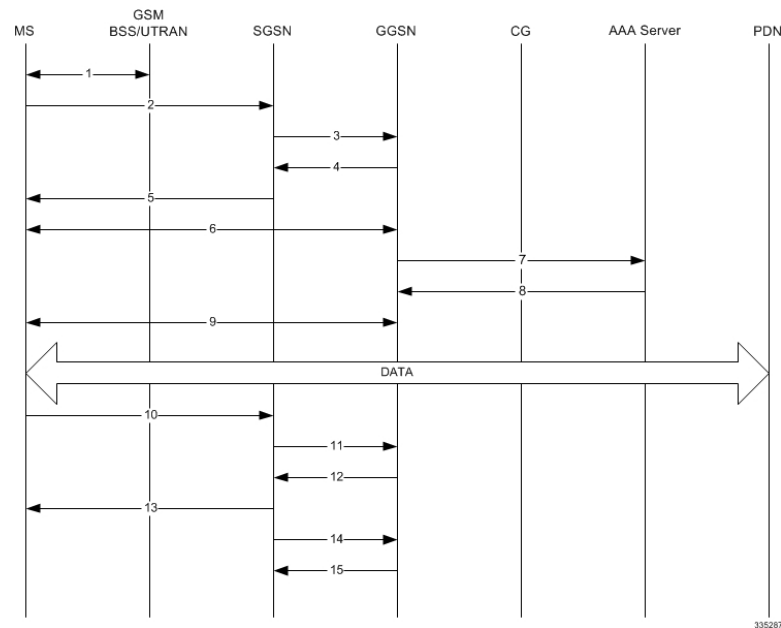
Upon PDP context establishment, the MS can send and receive data to or from the PDN until the session is closed or times out.

- 8 The MS can terminate the data session at any time. To terminate the session, the MS begins the PDP Context De-Activation procedure as described in *step 6* through *step 11* of the *Transparent Session IP Call Flow* section of this chapter.

PPP Direct Access Call Flow

The following figure and the text that follows describe the call flow for a successful PPP Direct Access data session.

Figure 11: PPP Direct Access Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 3 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
- 4 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines that the PDP context type is PPP and based on the APN, what authentication protocol to use and how to perform IP address assignment.
The GGSN replies with an affirmative Create PDP Context Response using GTPC.
- 5 The SGSN returns an Activate PDP Context Accept response to the MS.

- 6 The MS and the GGSN negotiate PPP.
- 7 The GGSN forwards authentication information received from the MS as part of PPP negotiation to the AAA server in the form of an Access-Request.
- 8 The AAA server authenticates the MS and sends an Access-Accept message to the GGSN.
- 9 The GGSN assigns an IP address to the MS and completes the PPP negotiation process. More information about IP addressing for PDP contexts is located in the *PDP Context Processing* and *Dynamic IP Address Assignment* sections of this chapter.

Once the PPP negotiation process is complete, the MS can send and receive data.

- 10 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 11 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
- 12 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
- 13 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 14 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 15 For each accounting message received from the GGSN, the CG responds with an acknowledgment.

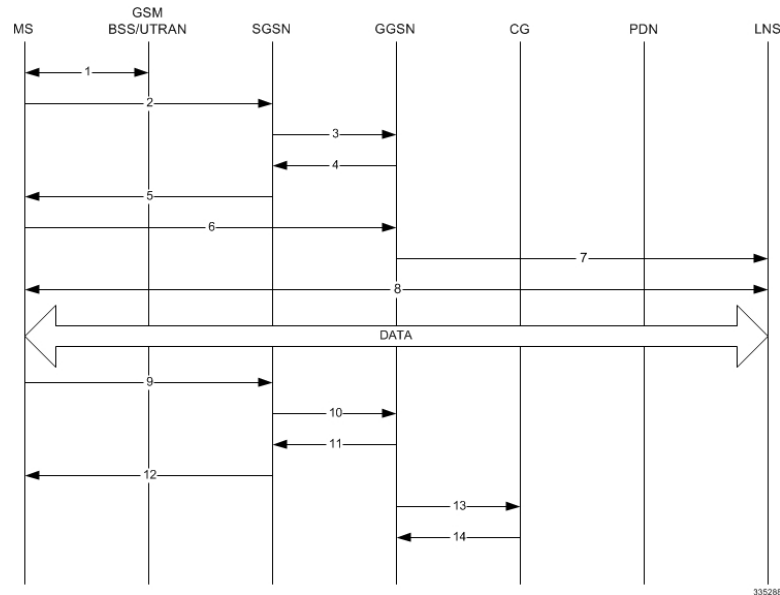
Limitations:

- Secondary PDP context creation for GGSN PDP type PPP session is not supported.
- PDP type PPP for GnGp GGSN is not supported.
- Routing Behind Mobile Station functionality for GGSN PDP-type PPP is not supported.
- Inter-Chassis session recovery of GGSN PDP-type PPP sessions is not supported.
- Multi-PDN with PDP-type PPP is not supported.
- Inter-RAT handovers with PDP-type PPP is not supported.
- L2TP with PDP-type PPP is not supported in this release.
- Lawful Interception with PDP-type PPP is not supported.
- Static IP address allocation with PDP-type PPP is not supported.
- IPv6 address allocation with PDP-type PPP is not supported.

Virtual Dialup Access Call Flow

The following figure and the text that follows describe the call flow for a successful VPN Dialup Access data session.

Figure 12: Virtual Dialup Access Call Flow



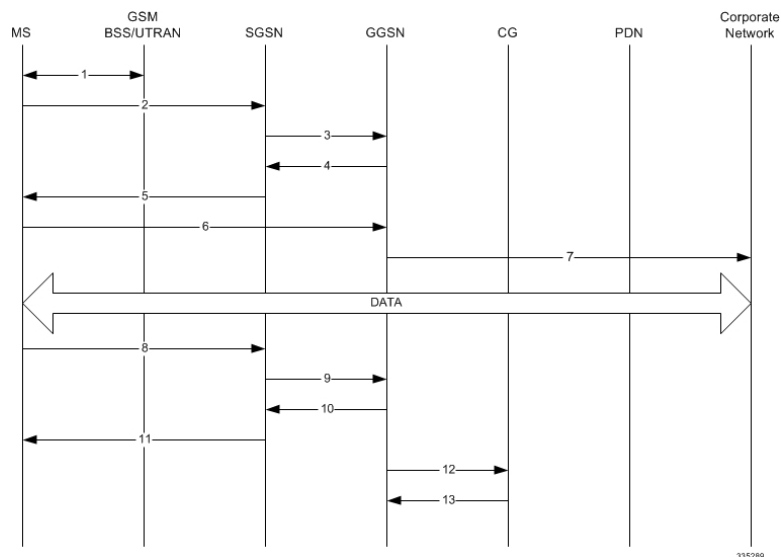
- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 3 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
- 4 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.
The GGSN replies with an affirmative Create PDP Context Response using GTPC.
- 5 The SGSN returns an Activate PDP Context Accept response to the MS.
- 6 The MS sends packets which are received by the GGSN.
- 7 The GGSN encapsulates the packets from the MS using L2TP and tunnels them to the LNS.
- 8 The LNS terminates the tunnel and un-encapsulates the packets.
The MS can send and receive data over the L2TP tunnel facilitated by the GGSN.

- 9 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 10 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
- 11 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
- 12 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 13 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 14 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Corporate IP VPN Connectivity Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 13: Corporate IP VPN Connectivity Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 3 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol).

The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.

- 4 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.

The GGSN replies with an affirmative Create PDP Context Response using GTPC.

- 5 The SGSN returns an Activate PDP Context Accept response to the MS.
- 6 The MS sends IP packets which are received by the GGSN.
- 7 The GGSN encapsulates the IP packets from the MS using IP-in-IP and tunnels them to the subscriber's corporate network.

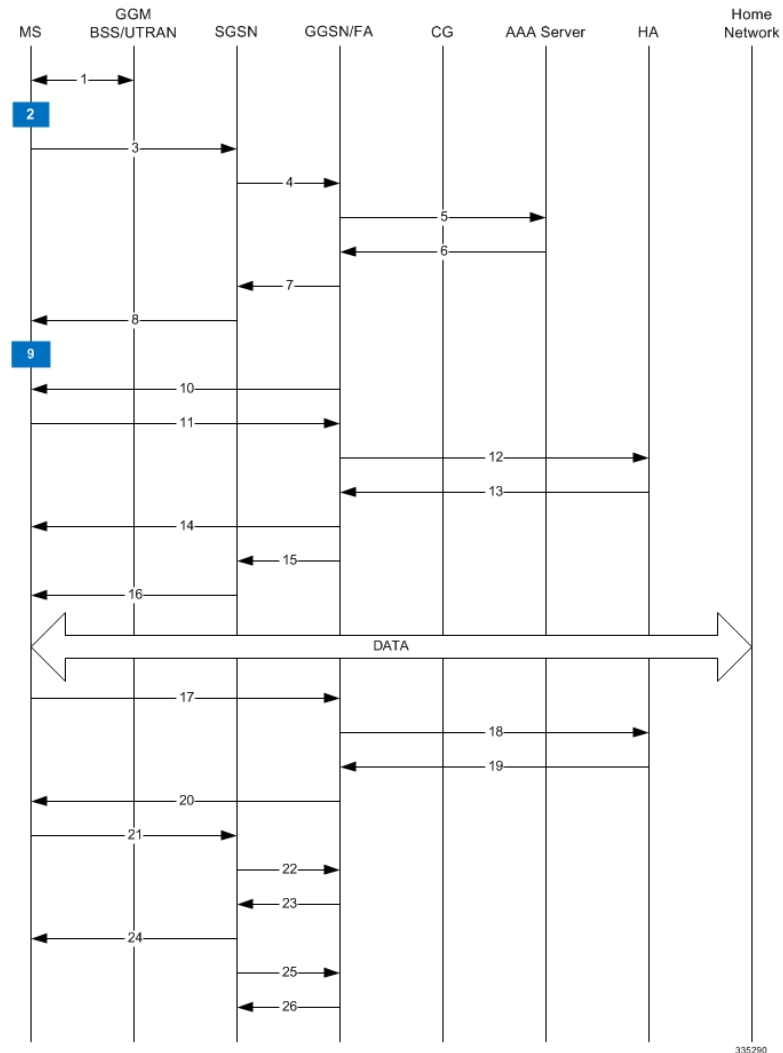
All data sent and received by the MS over the IP-in-IP tunnel facilitated by the GGSN.

- 8 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 9 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
- 10 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
- 11 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 12 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 13 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Mobile IP Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 14: Mobile IP Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP home address to use or request that one be dynamically assigned.

- 3 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

Note that regardless of whether or not the MS has a static address or is requesting a dynamic address, the "Requested PDP Address" field is omitted from the request when using Mobile IP.

- 4 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, Requested PDP con, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID).

- 5 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

From the APN specified in the message, the GGSN determines how to handle the PDP context including whether or not Mobile IP should be used.

If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

- 6 If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
- 7 The GGSN replies to the SGSN with a PDP Context Response using GTPC. The response will contain information elements such as the PDP Address, and PDP configuration options specified by the GGSN. Note that for Mobile IP, the GGSN returns a PDP Address of 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
- 8 The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
- 9 The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. This ends the PPP mode between the MT and TE components of the MS.

Data can now be transmitted between the MS and the GGSN.

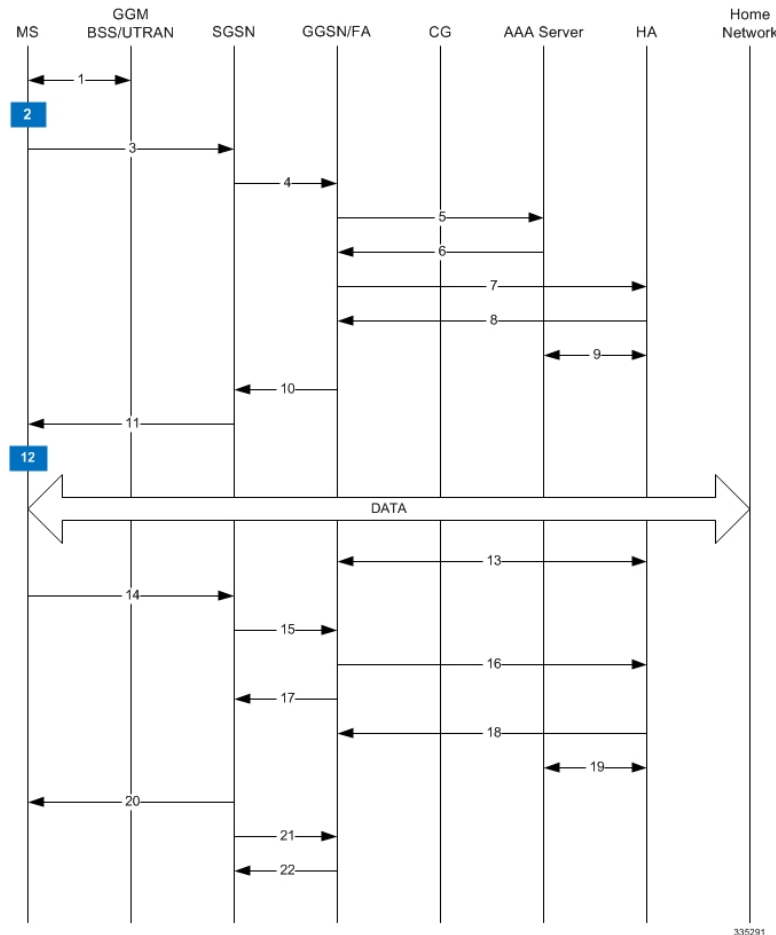
- 10 The FA component of the GGSN sends an Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more care-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
- 11 The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
- 12 The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN.
- 13 The HA sends a registration response to the FA containing the address assigned to the MS.

- 14 The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
- 15 The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
- 16 The SGSN forwards the PDP context modification message to the MS.
The MS can now send and receive data to or from their home network until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
- 17 The MS can terminate the Mobile IP data session at any time. To terminate the Mobile IP session, the MS sends a Registration Request message to the GGSN/FA with a requested lifetime of 0.
- 18 The FA component forwards the request to the HA.
- 19 The HA sends a Registration Reply to the FA accepting the request.
- 20 The GGSN/FA forwards the response to the MN.
- 21 The MS sends a Deactivate PDP Context Request message that is received by the SGSN.
- 22 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
- 23 The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN.
- 24 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 25 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 26 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Proxy Mobile IP Call Flows

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in which the MS receives its IP address from the HA.

Figure 15: HA Assigned IP Address Proxy Mobile IP Call Flow



- 1 The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
- 2 The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

- 3 The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
- 4 The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
- 5 The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.

Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings.

If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.
- 6 If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.
- 7 If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (Security Parameter Index (SPI)).
- 8 The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.
- 9 The HA sends a RADIUS Accounting Start request to the AAA server which the AAA server responds to.
- 10 The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
- 11 The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
- 12 The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

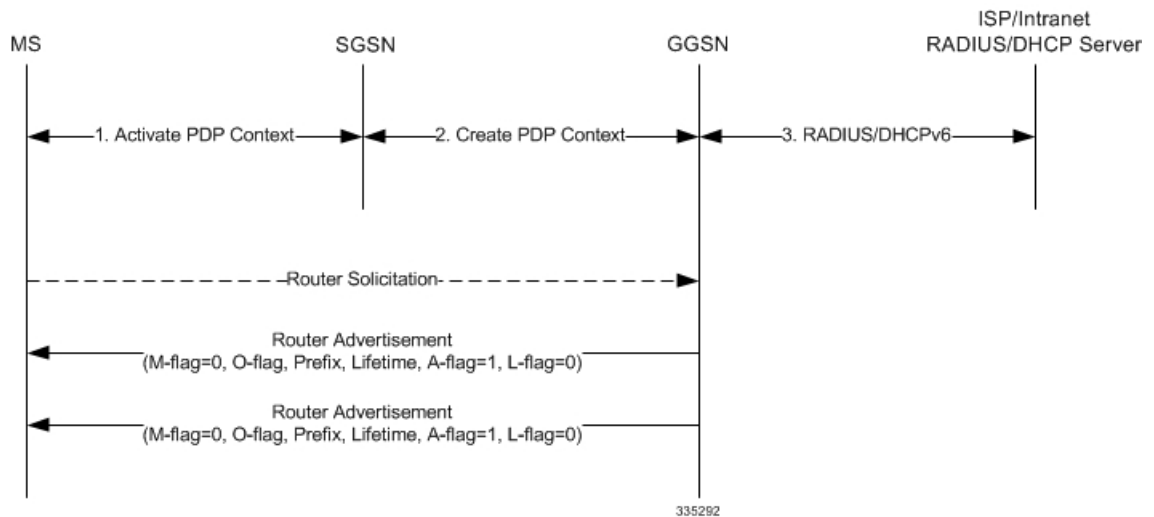
The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
- 13 The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
- 14 The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.

- 15 The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
- 16 The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
- 17 The GGSN returns a Delete PDP Context Response message to the SGSN.
- 18 The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
- 19 The HA sends a RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
- 20 The SGSN returns a Deactivate PDP Context Accept message to the MS.
- 21 The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
- 22 For each accounting message received from the GGSN, the CG responds with an acknowledgement.

IPv6 Stateless Address Auto Configuration Flows

The following figure and the text that follows describe a sample IPv6 stateless address auto configuration session setup call flow in which the MS receives its IP address from the RADIUS DHCP server.

Figure 16: IPv6 Stateless Address Auto Configuration Flow



- 1 The MS uses the IPv6 interface identifier provided by the GGSN to create its IPv6 link-local unicast address. Before the MS communicates with other hosts or mobile stations on the intranet/ISP, the MS must obtain an IPv6 global or site-local unicast address.
- 2 After the GGSN sends a create PDP context response message to the SGSN, it starts sending router advertisements periodically on the new MS-GGSN link established by the PDP context.

- 3 When creating a global or site-local unicast address, the MS may use the interface identifier received during the PDP context activation or it generates a new interface identifier. There is no restriction on the value of the interface identifier of the global or site-local unicast address, since the prefix is unique.

Supported Standards

The GGSN complies with the following standards for 3GPP wireless data services.

- [3GPP References, on page 69](#)
- [IETF References, on page 70](#)
- [Object Management Group \(OMG\) Standards, on page 73](#)

3GPP References

- 3GPP TS 09.60 v7.10.0 (2001-09): 3rd Generation Partnership project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 1998) for backward compatibility with GTPv0
- 3GPP TS 23.060 v7.6.0 (2007-9): 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 23.107 v7.1.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture
- 3GPP TS 23.203 V7.7.0 (2006-08): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 23.246 v7.4.0 (2007-09): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 7)
- 3GPP TS 24.008 v7.11.0 (2001-06): Mobile radio interface layer 3 specification; Core Network Protocols-Stage 3 (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 29.060 v7.9.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 4) for the Core GTP Functionality
- 3GPP TS 29.061 v7.7.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)
- 3GPP TS 29.212 v7.6.0 (2008-09) 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.5.0 (2005-08): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)

- 3GPP TS 29.281 V10.0.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 10)
- 3GPP TR 29.846 6.0.0 (2004-09) 3rd Generation Partnership Project, Technical Specification Group Core Networks; Multimedia Broadcast/Multicast Service (MBMS); CN1 procedure description (Release 6)
- 3GPP TS 32.015 v3.12.0 (2003-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging management; Call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- 3GPP TS 32.215 v5.9.0 (2005-06): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain (Release 5)
- 3GPP TS 32.251 v7.5.1 (2007-10) 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 7)
- 3GPP TS 32.298 v7.4.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299 v7.7.0 (2007-10): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 7)
- 3GPP TS 32.403 V7.1.0: Technical Specification Performance measurements - UMTS and combined UMTS/GSM
- 3GPP TS 33.106 V7.0.1 (2001-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 7)
- 3GPP TS 33.107 V7.7.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 7)

IETF References

- RFC-768, User Datagram Protocol (UDP), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991

- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996

- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile-IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol "L2TP", August 1999

- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- Draft, Route Optimization in Mobile IP
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

Object Management Group (OMG) Standards

CORBA 2.6 Specification 01-09-35, Object Management Group



Understanding the Service Operation

The system provides wireless carriers with a flexible solution for providing Gateway GPRS Support Node (GGSN) functionality for GPRS or UMTS networks.

The system functioning as a GGSN is capable of supporting the following types of subscriber data sessions:

- **Transparent IP:** The subscriber is provided basic access to a packet data network (PDN) without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDP) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscribers PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using a protocol such as IP-in-IP.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

- [Terminology, page 75](#)
- [How the System Selects Contexts, page 80](#)

Terminology

This section defines some of the terms used in the chapters that follow.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP interfaces, subscribers, etc. for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- **Source context:** Also referred to as the "ingress" context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a GPRS/UMTS network, the radio network containing the Service GPRS Support Nodes (SGSNs) would communicate with the system via Gn interfaces configured within the source context as part of the GGSN service.
- **Destination context:** Also referred to as the "egress" context, this context is where a subscriber is provided services (such as access to the Internet) as defined by access point name (APN) configuration templates. For example, the system's destination context would be configured with the interfaces facilitating subscriber data traffic to/from the Internet, a VPN, or other PDN.
- **Authentication context:** This context provides authentication functionality for subscriber PDP contexts and/or administrative user sessions and contains the policies and logical interfaces for communicating with Remote Authentication Dial In User Service (RADIUS) authentication servers.

For subscriber authentication, this functionality must be configured in the same system context as the APN template(s). Optionally, to simplify the configuration process, both subscriber RADIUS authentication functionality and APN templates can be configured in the destination context.



Important

To ensure scalability, authentication functionality for subscriber sessions should not be configured in the local context.

For administrative users, authentication functionality can either be configured in the local context or be authenticated in the same context as subscribers.

- **Accounting context:** This context provides accounting functionality for subscriber PDP contexts and/or administrative user sessions.

The system context in which accounting functionality is configured depends on the protocol used. Accounting for subscriber PDP contexts can be performed using either the GPRS Tunneling Protocol Prime (GTPP) or RADIUS. Accounting for administrative user sessions is based on RADIUS.

When using GTPP, it is recommended that accounting functionality be configured in a system source context along with the GGSN service.

When using RADIUS for subscriber accounting, it must be configured in the same context as RADIUS authentication. To simplify the configuration process, RADIUS-based authentication and accounting can be configured in a destination context as long as the APN templates are configured there as well.

RADIUS-based accounting for administrative user sessions can either be configured in the local context or in the same context used for subscriber accounting.



Important

To ensure scalability, accounting functionality for subscriber sessions should not be configured in the local context.

- **Local context:** This is the default context on the system used to provide out-of-band management functionality. The local context is described in the Command Line Reference.

Logical Interfaces

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a GGSN service, it will function as a Gn interface between the GGSN service and the SGSN. Services are defined later in this section.

There are several types of logical interfaces that must be configured to support the service as described below:

- **Gn:** This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signalling and data path for establishing and maintaining subscriber PDP contexts.

The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signalling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

One or more Gn interfaces can be configured per system context. Gn interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the four-port Quad Gig-E Line Card (QGLC).

- **Ga:** This is the interface used by the GGSN to communicate with the charging gateway (CG). The charging gateway is responsible for sending GGSN charging detail records (G-CDRs) received from the GGSN for each PDP context to the billing system.

The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

One or more Ga interfaces can be configured per system context. Ga interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gc:** This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signalling System 7 (SS7).

One Gc interface can be configured per system context. Gc interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gi:** This is the interface used by the GGSN to communicate with packet data networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

Additionally, inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

One or more Gi interfaces can be configured per system context. Gi interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gp:** This is the interface used by the GGSN to communicate with GPRS support nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

One or more Gn/Gp interfaces can be configured per system context. Gp interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **AAA:** This is the interface used by the GGSN to communicate with either an authentication or accounting server on the network using the Remote Authentication Dial In User Service (RADIUS) protocol.

This is an optional interface that can be by the GGSN for subscriber PDP context authentication or accounting. AAA interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **S6b:** This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.



Important

This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* in guide.

- **DHCP:** This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured to dynamically provide IP addresses for PDP contexts from the DHCP server.

DHCP interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

Bindings

A binding is an association between "elements" within the system. There are two types of bindings: static and dynamic.

Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.

- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a GGSN service bound to a logical interface will cause the logical interface to take on the characteristics of a Gn interface within a GPRS/UMTS network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Services

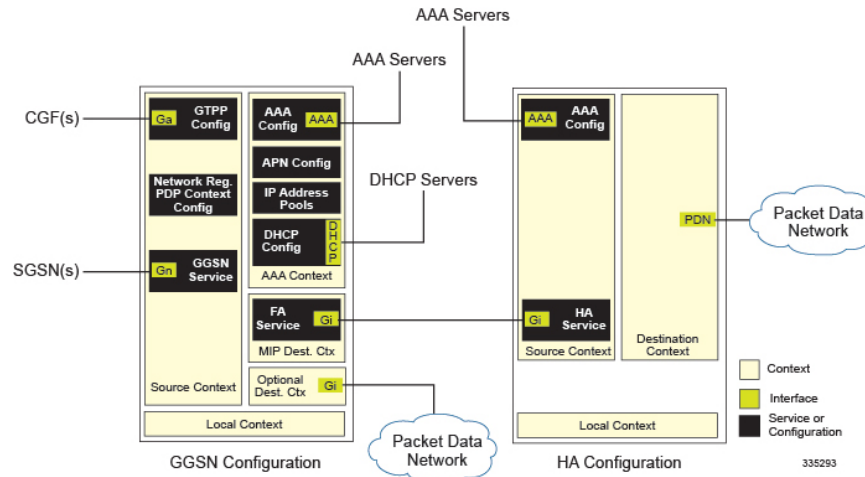
Services are configured within a context and enable certain functionality. The following services can be configured on the system:

- **GGSN services:** GGSN services are configured to support both mobile-initiated and network-requested PDP contexts. The GGSN service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of a Gn interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Gn interfaces.
- **FA services:** FA services are configured to support Mobile IP and define FA functionality on the system. The system supports multiple Mobile IP configurations. A single system can perform the function of a FA only, an HA only, or a combined PDSN/FA/HA. Depending on your configuration, the FA service can create and maintain the Pi interface between the PDSN/FA and the HA or it can communicate with an HA service configured within the same context.

The FA service should be configured in a different context from the PDSN service. However, if the FA service will be communicating with an HA that is a separate network element, it must be configured within the same context as and be bound to the Pi interfaces that allow it to communicate with the HA.
- **LAC services:** LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within networks to provide secure tunneling to an L2TP network server (LNS) on a remote PDN.
- **DHCP services:** DHCP services are configured on a system to provide dynamic assignment of IP address to PDP contexts through the use of the Dynamic Host Configuration Protocol (DHCP).

Following figure illustrates the relationship between services, interfaces, and contexts within the system for GPRS/UMTS networks.

Figure 17: Service, Interface, and Context Relationship Within the System for GPRS/UMTS Networks



The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system.

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.

How the System Selects Contexts

This section provides details about the process that is used to determine which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces need to be configured.

Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system.

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.



GGSN Service Configuration Procedures

This chapter is meant to be used in conjunction with the previous chapter that describes the information needed to configure the system to support GGSN functionality for use in GPRS/UMTS networks.

It is recommended that you identify the options from the previous chapters that are required for your specific deployment. You can then use the procedures in this chapter to configure those options.



Important

At least one Packet Accelerator Card (PAC) or Packet Services Card (PSC) must be made active prior to service configuration. Information and instructions for configuring PACs/PSCs to be active can be found in the Configuring System Settings chapter of the System Administration Guide.



Caution

While configuring any base-service or enhanced feature, it is highly recommended to take care of conflicting or blocked IP addresses and port numbers for binding or assigning. In association with some service steering or access control features, like *Access Control List* configuration, use of inappropriate port number may result in communication loss. Refer respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external network.

- [GGSN Service Configuration, page 84](#)
- [GTPP Accounting Support Configuration, page 87](#)
- [APN Configuration, page 90](#)
- [DHCP Service Configuration, page 96](#)
- [DHCPv6 Service Configuration, page 99](#)
- [DNS Configuration for IPv4v6 PDP Context, page 103](#)
- [IP Address Pool Configuration on the System, page 104](#)
- [Gn-Gp Handoff Support Configuration, page 107](#)
- [FA Services Configuration, page 110](#)
- [Common Gateway Access Support Configuration, page 114](#)
- [Rf Interface Configuration for Offline Charging, page 117](#)

- [Configuring RFL Bypass Feature, page 119](#)

GGSN Service Configuration

GGSN services are configured within contexts and allow the system to function as a GGSN in the either a GPRS or UMTS wireless data network.



Important

This section provides the minimum instruction set for configuring a GGSN service that allows the system to process PDP contexts. Commands that configure additional GGSN service properties are provided in the *GGSN Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*.

To configure the system to work as GGSN service:

-
- Step 1** Create the GGSN service, local User Datagram Protocol (UDP) port for the Gn interfaces' IP socket, and bind it to an IP address by applying the example configuration in the *GGSN Service Creation and Binding* section.
 - Step 2** Associate the accounting context for the GGSN service and configure charging characteristic profile parameters for GGSN service by applying the example configuration in the *Accounting Context and Charging Characteristics Configuration* section.
 - Step 3** Configure the SGSN and PLMN related policy and session setup timeout for the GGSN service by applying the example configuration in the *SGSN and PLMN Policy Configuration* section.
 - Step 4** Optional. Configure the GGSN service to support network-requested PDP contexts by applying the example configuration in the *Network-requested PDP Context Support Configuration* section.
 - Step 5** Verify your GGSN configuration by following the steps in the *GGSN Configuration Verification* section.
 - Step 6** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
-

GGSN Service Creation and Binding

Use the following example to create the GGSN service and bind it to an IP address:

```
configure
  context <vpn_ctxt_name> -noconfirm
    ggsn-service <ggsn_svc_name>
  end
```

Notes:

- A maximum of 256 services (regardless of type) can be configured per system.
- Bind address should not conflict with any other GTP-based service.

Accounting Context and Charging Characteristics Configuration

Use the following example to configure a GTPP accounting context and charging characteristics parameters for GGSN service.

```
configure
context <vpn_ctxt_name>
  ggsn-service <ggsn_svc_name>
  accounting context <aaa_ctxt_name>

  cc profile <cc_prof_index>
end
```

Notes:

- Charging characteristics behavior and profile index can be configured for multiple CC profile indexes. For more options and keywords like **buckets**, **interval**, **sgsns**, **tariff**, **volume** etc., refer cc profile section in Command Line Interface Reference.
- This command works in conjunction with the **cc-sgsn** command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts. Refer to the *APN Configuration* section in this chapter.

SGSN and PLMN Policy Configuration

Use the following example to configure the SGSN and PLMN related policy and session setup timeout for the GGSN service:

```
configure
context <vpn_ctxt_name>
  ggsn-service <ggsn_svc_name>
    plmn id mcc <mcc_number> [ mnc <mnc_number> ] [primary]
    sgsn address <ip_address> / <subnet_mask>
    plmn unlisted-sgsn [foreign | home | reject]
    setup-timeout <dur_sec>
  end
```

Notes:

- SGSN or PLMN related policy can be defined for multiple SGSNs or PLMN.
- For optional configuration parameters of SGSN address, refer Command Line Interface Reference.



Important

The GGSN only communicates with the SGSNs configured using this command unless a PLMN policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-sgsn** command.

Network-requested PDP Context Support Configuration

Use the following example to configure the GGSN to support the network-requested PDP context:

```
configure
    context <vpn_ctxt_name>
        network-requested-pdp-context activate <ip_address> dst-context <dst_ctxt_name> imsi
        <imsi> apn <apn_name>
        network-requested-pdp-context gsn-map <ip_address>
    end
```

Notes:

- It is recommended that this functionality be configured in the system source context(s) along with the GGSN service(s).
- Up to 1000 IP address can be configured for network request PDP context support.
- Only one GSN-MAP node can be configured per system context.

GGSN Configuration Verification

Step 1

Verify that your GGSN services were created and configured properly by entering the following command in Exec Mode:

show ggsn-service name <ggsn_svc_name>}

The output of this command given below is a concise listing of GGSN service parameter settings as shown in the sample output displayed. In this example, a GGSN service called *ggsn1* was configured and you can observe some parameters configured as default.

```
Service name:                               ggsn1
Context:                                     ggsn1
Associated PGW svc:                         None
Associated GTPU svc:                       None
Accounting Context Name: ggsn1
dns-client Context Name:
Authorize:                                 Disabled
Fqdn-name:                                Disabled
Bind:                                     Done
Local IP Address:                          192.168.70.1      Local IP Port: 2123
Self PLMN Id.:                            MCC: 450, MNC: 06
Retransmission Timeout: 20 (secs)
Max Retransmissions: 4
Restart Counter: 16
Echo Interval: 60 (secs)
```

```
Guard Interval: 100 (secs)
Setup Timeout: 60 (secs)
PLMN Policy: Reject unlisted SGSN
Reject Code Policy:
    Authentication Server Timeout: User Authentication Failed
    Accounting Server Timeout: No Resources Available
Ran Procedure Ready: Disabled
NSAPI in Create PDP response: Disabled
Duplicate Subscriber Addr Request: Reject
trace-collection-entity: Disabled
Path Failure Detection on gtp msgs: Echo
GTP Private Extensions:
```

```

None
Max IP sessions:          4000000
Max PPP sessions:        2500000
Max sessions:            4000000
Service Status:          Started
Newcall Policy:          None
MBMS Policy:              None
MBMS Charging ID Optimization: Disabled

3GPP Qos to DSCP Mapping (for G-PDUs):
qci 1:                    ef
qci 2:                    ef
qci 3:                    af11
qci 4:                    af11
qci 5:                    ef
qci 6:                    ef
qci 7:                    af21
qci 8:                    af21
qci 9:                    be

3GPP Qos to DSCP Mapping based on Alloc. Prio:
qci 5 (Alloc. P 1):      ef
qci 5 (Alloc. P 2):      ef
qci 5 (Alloc. P 3):      ef
qci 6 (Alloc. P 1):      ef
qci 6 (Alloc. P 2):      ef
qci 6 (Alloc. P 3):      ef
qci 7 (Alloc. P 1):      af21
qci 7 (Alloc. P 2):      af21
qci 7 (Alloc. P 3):      af21
qci 8 (Alloc. P 1):      af21
qci 8 (Alloc. P 2):      af21
qci 8 (Alloc. P 3):      af21
GTPC messages:          be
Background:              be
Charging Characteristics(CC) Behaviors:
No records (Bit No.):    0
Charging Characteristics(CC) Profiles:
Profile 0:
  Buckets: 4              SGSN changes: 4
Profile 1:
  Buckets: 4              SGSN changes: 4
SGSN Configuration List:
sgsn address 2.2.2.2/32 mcc 111 mnc 999 description aaa-ggsn

```

Step 2

Verify configuration for errors by entering the following command in Exec Mode:
show configuration errors section ggsn-service verbose

GTPP Accounting Support Configuration

This section provides instructions for configuring GTPP-based accounting for subscriber PDP contexts. GTPP-based accounting for a subscriber can be configured by CGF server configuration in a GTPP group. Additionally individual CGF server can be configured with this example.

For information on configuring Diameter and RADIUS AAA functionality, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends.

GTPP version 2 is used by default. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. For CDR encoding different dictionaries are supported.

For more information on GTPP dictionaries, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *GTPP Interface Administration and Reference*.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. However it accepts charging characteristics from RADIUS too, they must always be provided by the SGSN for GTPPv1 requests for primary and secondary PDP contexts.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level (refer to the *APN Configuration* section of this chapter for more information). GGSN charging characteristics consist of a profile index and behavior settings (refer to the *GGSN Service Configuration* section of this chapter for more information). The profile indexes specify the criteria for closing accounting records based specific criteria (refer to the *GGSN Service Configuration* section of this chapter for more information).



Important

This section provides the minimum instruction set for configuring a GTPP accounting support in a GGSN service. Commands that configure additional GTPP accounting properties are provided in the *Command Line Interface Reference* guide.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the GTPP accounting support for a GGSN service:

-
- Step 1** Create the GTPP group in accounting context by applying the example configuration in the *GTPP Group Creation* section.
 - Step 2** Configure the charging agent and GTPP server (CGF) related parameters for the GTPP accounting support by applying the example configuration in the *GTPP Group Configuration* section.
 - Step 3** Verify your GTPP group and accounting configuration by following the steps in the *GTPP Group Configuration Verification* section.
 - Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
-

GTPP Group Creation

Use the following example to create the GTPP group to support GTPP accounting:

```
configure
    context <vpn_ctxt_name>
        gtp group <gtp_group_name> -noconfirm
    end
```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.

GTPP Group Configuration

Use the following example to configure the GTPP server parameters, GTPP dictionary, and optionally CGF to support GTPP accounting:

configure

```

context <vpn_ctxt_name>
  gtp group <gtp_group_name>
    gtp charging-agent address <ip_address> [port <port>]
    gtp server <ip_address> [max <msgs >] [priority <priority>]
    gtp dictionary <dictionaries>
    gtp max-cdrs <number_cdrs> [wait-time <dur_sec>]
    gtp transport-layer {tcp | udp}
  end

```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.
- Command for CGF **gtp charging-agent** is optional and configuring gtp charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address. Multiple interfaces can be configured within a single context if needed.
- For more information on GTPP dictionary encoding, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *GTPP Interface Administration and Reference*.
- For better performance, it is recommended to configure maximum number of CDRs as 255 with **gtp max-cdrs** command.
- Operator can select transport layer protocol as TCP or UDP for Ga interface with **gtp transport-layer** command.
- Multiple GTPP server can be configured using multiple instances of this command subject to following limits:
 - Total 4 GTPP server in one GTPP group
 - Total 32 GTPP server in one context or in the overall configuration

- Total 33 GTPP groups (1 default and 32 user defined GTPP groups) can be configured in one context. Number of CGFs in 1 GTPP group is limited to 4 and a total of 32 CGF servers across all GTPP groups in one context are configurable.
- Total 32 GTPP groups can also be configured under an APN

GTPP Group Configuration Verification

Step 1 Verify that your CGFs were configured properly by entering the following command in Exec Mode:

show gtp accounting servers

This command produces an output similar to that displayed below:

context:	source					
Preference	IP		Port	Priority	State	Group
Primary	192.168.32.135	3386	1		Active	default
Primary	192.168.89.9	3386	100		Active	default

Step 2 Verify configuration for errors by entering the following command in Exec Mode:

show configuration errors section ggsn-service verbose

APN Configuration

This section provides instructions for configuring the APN templates that are used to determine how PDP contexts should be processed. APNs are configured in system authentication contexts.



Important

This section provides the minimum instruction set for configuring APNs in a GGSN service. Commands that configure additional APN properties are provided in *APN Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in the *GGSN Service Configuration* section of this guide.

To configure the APN properties for a GGSN service:

-
- | | |
|---------------|---|
| Step 1 | Create the APN in system context and specify the support of PDP contexts and selection mode by applying the example configuration in the APN Creation and Configuration section. |
| Step 2 | Configure the authentication and accounting parameters in APN by applying the example configuration in the Authentication, Accounting, and GTP Group Configuration in APN section. |
| Step 3 | Configure the IP allocation method in APN by applying the example configuration in the IP Address Allocation Method Configuration in APN section. |
| Step 4 | Optional. Configure the charging characteristics related parameters for the APN by applying the example configuration in the Charging Characteristics Parameter Configuration in APN section. |
| Step 5 | Optional. Configure virtual APNs by applying the example configuration in the Virtual APN Configuration section. |
| Step 6 | Optional. Configure other optional parameters for the APN by applying the example configuration in the Other Optional Parameter Configuration in APN section. |
| Step 7 | Verify your APN configuration by following the steps in the APN Configuration Verification section. |
| Step 8 | Save your configuration as described in the <i>Verifying and Saving Your Configuration</i> chapter. |
-

APN Creation and Configuration

Use the following example to create and configure the APNs:

```
configure
context <vpn_ctxt_name>
  apn <apn_name> -noconfirm
  pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}
  selection-mode {sent-by-ms | chosen-by-sgsn | subscribed}
  ip context-name <dst_ctxt_name>
end
```

Notes:

- Up to 2,048 APNs can be configured on a system.
- APN templates should be created/configured within system authentication contexts or destination context.
- Selection mode parameter's setting must be identical to the selection mode setting on the SGSN(s) that the GGSN communicates with. The GGSN rejects attempts to establish PDP contexts from any SGSN having a different setting.
- For IPv6 calls to work, the destination context must have an IPv6 interface configured in it.
- If the APN supports Mobile IP for subscriber PDP contexts, then ip context-name command is used to indicate the context in which the FA service is configured.
 - If no context name is specified, the system uses the context in which the APN is configured.
 - If Mobile IP is supported and no name is specified, the system uses the context in which the GGSN service facilitating the PDP context is located.

Authentication, Accounting, and GTPP Group Configuration in APN

This section describes the procedure to configure the authentication and accounting parameters for an APN. It also specifies the procedure to attach a GTPP group with an APN.

-
- Step 1** Configure the authentication and accounting parameters by applying the example configuration in the *Authentication and Accounting Configuration in APN* section.
- Step 2** Attach a GTPP group with APN by applying the example configuration in the *GTPP Group Association to APN* section.
-

Authentication and Accounting Configuration in APN

Use the following example to configure the accounting mode and authentication parameter for APN:

```
configure
    context <dst_ctxt_name>
    apn <apn_name>
        accounting-mode {none | gtp | radius [no-interims] [no-early-pdus]}
        default authentication
    end
```

Notes:

- APNs are configured in system authentication contexts or destination context.
- The authentication process varies depending on whether the PDP context is of type IP or PPP. The **authentication** command provides **imsi-auth**, **msisdn-auth**, **eap initial-access-request**, **allow-noauth**, **chap**, **mschap**, and **pap** options. For more information on type of authentication, refer authentication section in APN Configuration Mode Commands chapter of Command Line Interface Reference.

GTPP Group Association to APN

After configuring GTPP group at context-level, an APN within the same context can be configured to use the user defined GTPP group.

Refer section *GTPP Accounting Support Configuration* for GTPP group configuration.

```
configure
    context <vpn_ctxt_name>
    apn <apn_name>
        gtp group <gtp_group_name> [accounting-context <aaa_ctxt_name>]
    end
```

Notes:

- GTPP group must be configured before associating with APN or "default" GTPP group can be used.

IP Address Allocation Method Configuration in APN

Use the following example to configure the IP address allocation method for APN:

**Important**

Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

configure

```

    context <dst_ctxt_name>
    apn <apn_name>
    ip address alloc-method { dhcp-proxy [allow-deferred] [prefer-dhcp-options] | dhcp-relay
| local [allow-deferred] | no-dynamic [allow-deferred] } [allow-user-specified]
    end

```

Notes:

- The process used by the system to determine how the address should be allocated. For detail information on IP address allocation, refer Usage section of **ip address alloc-method** command in *APN Configuration Mode Commands* chapter of Command Line Interface Reference.
- If DHCP-Proxy and DHCP-Relay method is selected for IP address allocation, a DHCP service must be configured on the system as described in *DHCP Service Configuration* section and specified the name of DHCP Service by entering the **dhcp service-name** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.
- If local pool is selected for IP address allocation, a local pool must be configured on the system as described in *IP Address Pool Configuration on the System* section and specified the name of a private IP address pool by entering the **ip address pool** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

Charging Characteristics Parameter Configuration in APN

Use the following example to configure the charging characteristics parameter for APN:

**Important**

Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

configure

```

    context <dst_ctxt_name>
    apn <apn_name>
    cc-sgsn {home-subscriber-use-GGSN | roaming-subscriber-use-GGSN |
visiting-subscriber-use-GGSN}+
    cc-home behavior <bit> profile <index>
    cc-roaming behavior <bit> profile <index>
    cc-visiting behavior <bit> profile <index>
    end

```

Notes:

- If multiple behavior bits are configured for a single profile index, the variable bits is achieved by "Or"ing the bit strings and converting the result to hexadecimal.

Example

If behavior bits 5 (0000 0001 0000) and 11 (0100 0000 0000) are both being assigned to profile index 5 for a home subscriber, the appropriate command is **cc-home behavior 410 profile 5**.

Virtual APN Configuration

Virtual APNs are references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. Use the following example to configure the virtual APNs.

configure

```

    context <dst_ctxt_name>
        apn <apn_name>
virtual-apn preference priority apn apn_name [ access-gw-address { ip_address | ip_address/mask } |
bearer-access-service service_name | cc-profile cc_profile_index [ pre-rel-9.1-cc-behavior cc_behavior_value
]| rat-type { eutran | gan | geran | hspa | utran | wlan } ] | cc-behavior cc_behavior_value [ rat-type {
eutran | gan | geran | hspa | utran | wlan } ] | domain domain_name | mcc mcc_number mnc mnc_number
| cc-profile cc_profile_index [ pre-rel-9.1-cc-behavior cc_behavior_value ] | cc-behavior cc_behavior_value
| msin-range from msin_range_from to msin_range_to | rat-type { eutran | gan | geran | hspa | utran
| wlan } ] | msisdn-range from msisdn_start_range to msisdn_to_range | rat-type { eutran | gan | geran |
hspa | utran | wlan } ] | pdp-type { ipv4 | ipv6 | ipv4v6 } | roaming-mode { roaming } ] | rat-type { eutran
| gan | geran | hspa | utran | wlan } | roaming-mode { home | roaming | visiting } ] ]
end

```

Notes:

- Up to 1023 references can be configured per APN. Additional information about "virtual" APNs and their operation can be found in the *Command Line Interface Reference*.

Other Optional Parameter Configuration in APN

Use the following example to configure various optional parameter for APN:

configure

```

    context <dst_ctxt_name>
        apn <apn_name>
            dns {primary | secondary} {<dns_ip_address>}
            mobile-ip required
            mobile-ip home-agent <ha_ip_address>
            ip source-violation {ignore | check [drop-limit <limit>]} [exclude-from-accounting]
            restriction-value <value>
            timeout {absolute | idle | qos-renegotiate} <timeout_dur>
            timeout long-duration <ldt_dur> [inactivity-time <inact_dur>]
            long-duration-action detection
            long-duration-action disconnection [suppress-notification] [dormant-only] +
        end
    end

```

Notes:

- Mobile is supported for IP PDP contexts only. Mobile IP configuration attributes returned as part of a successful authentication during the GTP authentication phase (for non-transparent IP PDP contexts) supersede the APN configuration. Any attributes returned during the FA authentication phase are ignored.
- If mobile-ip required option is enabled, the system deletes any PDP context using the APN that can not establish a Mobile IP session.

APN Configuration Verification

Step 1

Verify that your APN were configured properly by entering the following command in Exec Mode:

show apn all

This command produces an output similar to that displayed below is an excerpt from a sample output. In this example, an APN called *apn1* was configured.

```

access point name (APN):      apn1
authentication context:      test
pdp type:                    ipv4
ehrpdp access:               N/A
Selection Mode:              subscribed
ip source violation:          Checked
accounting mode: gtpdp
no-interims:                 Disabled
Bearer Control Mode:         none
max-primary-pdp-contexts:    1000000
current primary-pdp-contexts: 0
primary contexts:            not available
max secondary contexts per-subscriber: 10
Credit Control:              disabled
mbms bearer absolute timeout: 0
mbms ue absolute timeout:    0
permission:
  local ip:                   0.0.0.0
  primary dns:                0.0.0.0
  primary nbns:               0.0.0.0
  ppp keep alive period :     0
  absolute timeout :          0
  idle-timeout-activity ignore-downlink: Disabled
  long duration timeout:      0
  long duration action:       Detection
  wimax header compression/suppression: none
  ip header compression:      vj
  ip hide service address:     Disabled
  ip output access-group:
  ipv6 output access-group:
  policy-group in:
  permit ip multicast:         False
  ppp authentication:
  eap authentication initial-access-request: authenticate-authorize
  allow noauthentication:       Enabled
  msisdn authentication:        Disabled
  ip destination context:      ip-ctx
  Rule Base:                   default
  FW-and-NAT Policy:           default
  Bandwidth-Policy:            default
  Link-Monitoring:             OFF
  Content-Filtering Policy-Id:  Not configured
  mediation accounting:        Disabled
  mediation-device context:     Not set
  mediation no-interims:        Disabled
  outbound username:           N/A
  ip address pools:            N/A
  ip address secondary pools:   N/A
  access-link ip-frag:         df-ignore
  ignore DF-bit data-tunnel:    On
  ip allocation type:           local pool
  prefer dhcp options:          false
  allow deferred:               true
  3GPP Qos to DSCP Mapping:
    qci 1:                      ef
    qci 2:                      ef
    qci 3:                      af11
    qci 4:                      af11
drop limit:                  10
No early PDUs: Disabled
total-pdp-contexts:         1000000
total-pdp-contexts:         0
total contexts: not available
IMS Authorization:           disabled
mbms bearer idle timeout:    0
next hop gateway addr:
  secondary dns:              0.0.0.0
  secondary nbns:             0.0.0.0
  ppp mtu :                   1500
  idle timeout :              0
long dur inactivity time:    Disabled
ip input access-group:
ipv6 input access-group:
policy-group out:
mediation no early PDUs:     Disabled
mediation delay-GTP-response: Disabled
allow user specified ip addr: true

```

```

qci 5:          ef
qci 6:          ef
qci 7:          af21
qci 8:          af21
qci 9:          be
3GPP Qos to DSCP Mapping based on Alloc. Prio:
qci 5 (Alloc. P 1):  ef
qci 5 (Alloc. P 2):  ef
qci 5 (Alloc. P 3):  ef
qci 6 (Alloc. P 1):  ef
qci 6 (Alloc. P 2):  ef
qci 6 (Alloc. P 3):  ef
qci 7 (Alloc. P 1):  af21
qci 7 (Alloc. P 2):  af21
qci 7 (Alloc. P 3):  af21
qci 8 (Alloc. P 1):  af21
qci 8 (Alloc. P 2):  af21
qci 8 (Alloc. P 3):  af21
GTPP Group:      gtpg-gp          GTPP Accounting Context:  acc
Mobile IPv6 Tunnel MTU:  1500
Mobile IPv6 Tunnel MTU Exceed Action:  notify-sender
Mobile IPv6 Home Agent:  none
Mobile IPv6 Home Link Prefix:  ::/0
Mobile IPv6 Home Address:  none

```

Step 2 Verify configuration for errors in APN configuration by entering the following command in Exec Mode:
show configuration errors section ggsn-service verbose

DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using one of two methods as configured within an APN:

- **DHCP-proxy:** The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

- **DHCP-relay:** The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

Regardless of the DHCP method, there are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.

**Important**

This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer DHCP Service Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the DHCP service:

-
- Step 1** Create the DHCP service in system context and bind it by applying the example configuration in the *DHCP Service Creation* section.
 - Step 2** Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the *DHCP Server Parameter Configuration* section.
 - Step 3** Verify your DHCP Service configuration by following the steps in the *DHCP Service Configuration Verification* section.
 - Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
-

DHCP Service Creation

Use the following example to create the DHCP service to support DHCP-based address assignment:

configure

```

    context <dest_ctxt_name>
        dhcp-service <dhcp_svc_name>
            bind address <ip_address> [nexthop-forwarding-address <nexthop_ip_address>
[mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]]]
            end

```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address <nexthop_ip_address> [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [out_mpls_label_value2]]** applies DHCP over MPLS traffic.

DHCP Server Parameter Configuration

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

configure

```

    context <dest_ctxt_name>
        dhcp-service <dhcp_svc_name>
            dhcp server <ip_address> [priority <priority>]
            dhcp server selection-algorithm {first-server | round-robin}

```

```

lease-duration min <minimum_dur> max <max_dur>
dhcp deadtime <max_time>
dhcp detect-dead-server consecutive-failures <max_number>
max-retransmissions <max_number>
retransmission-timeout <dur_sec>
end

```

Notes:

- Multiple DHCP services can be configured. Each service can have multiple DHCP servers configured by entering **dhcp server** command multiple times. A maximum of 225 DHCP services can be configured with maximum of 8 DHCP servers configurations per DHCP service.
- The **dhcp detect-dead-server** command and **max-retransmissions** command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with **max-retransmissions** command.

DHCP Service Configuration Verification

Step 1 Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

show dhcp service all

This command produces an output similar to that displayed below where DHCP name is *dhcp1*:

```

Service name:                dhcp1
Context:                     isp
Bind:                        Done
Local IP Address:            150.150.150.150
Next Hop Address:            192.179.91.3
MPLS-label:
Input:                        5000
Output:                      1566 1899
Service Status:              Started
Retransmission Timeout:      3000 (milli-secs)
Max Retransmissions:         2
Lease Time:                  600 (secs)
Minimum Lease Duration:      600 (secs)
Maximum Lease Duration:      86400 (secs)
DHCP Dead Time:              120 (secs)
DHCP Dead consecutive Failure:5
DHCP T1 Threshold Timer:     50
DHCP T2 Threshold Timer:     88
DHCP Client Identifier:      Not Used
DHCP Algorithm:              Round Robin
DHCP Servers configured:
Address: 150.150.150.150      Priority: 1
DHCP server rapid-commit:    disabled
DHCP client rapid-commit:    disabled
DHCP chaddr validation:      enabled

```

Step 2 Verify the DHCP service status by entering the following command in Exec Mode:

show dhcp service status

DHCPv6 Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) for IPv6 to enable the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and APN as described in *APN Configuration* section of this chapter.

To configure the DHCPv6 service:

-
- | | |
|---------------|--|
| Step 1 | Create the DHCPv6 service in system context and bind it by applying the example configuration in the <i>DHCPv6 Service Creation</i> section. |
| Step 2 | Configure the DHCPv6 server and other configurable values for Renew Time, Rebind Time, Preferred Lifetime, and Valid Lifetime by applying the example configuration in the <i>DHCPv6 Server Parameter Configuration</i> section. |
| Step 3 | Configure the DHCPv6 client and other configurable values for Maximum Retransmissions, Server Dead Tries, and Server Resurrect Time by applying the example configuration in the <i>DHCPv6 Client Parameter Configuration</i> section. |
| Step 4 | Configure the DHCPv6 profile by applying the example configuration in the <i>DHCPv6 Profile Configuration</i> section. |
| Step 5 | Associate the DHCPv6 profile configuration with the APN by applying the example configuration in the <i>Associate DHCPv6 Configuration</i> section. |
| Step 6 | Verify your DHCPv6 Service configuration by following the steps in the <i>DHCPv6 Service Configuration Verification</i> section. |
| Step 7 | Save your configuration as described in the <i>Verifying and Saving Your Configuration</i> chapter. |
-

DHCPv6 Service Creation

Use the following example to create the DHCPv6 service to support DHCP-based address assignment:

```
configure
    context <dest_ctxt_name>
        dhcpv6-service <dhcpv6_svc_name>
            bind address <ipv6_address> port <port>
        end
```

Notes:

- To ensure proper operation, DHCPv6 functionality should be configured within a destination context.
- The Port specifies the listen port and is used to start the DHCPv6 server bound to it. It is optional and if unspecified, the default port is 547.

DHCPv6 Server Parameter Configuration

Use the following example to configure the DHCPv6 server parameters to support DHCPv6-based address assignment:

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-server
        renew-time <renewal_time>
        rebind-time <rebind_time>
        preferred-lifetime <pref_lifetime>
        valid-lifetime <valid_lifetime>
      end
    end
```

Notes:

- Multiple DHCP can be configured by entering **dhcp server** command multiple times. A maximum of 256 services (regardless of type) can be configured per system.
- **renew-time** configures the renewal time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **rebind-time** configures the rebind time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **preferred-lifetime** configures the preferred lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.
- **valid-lifetime** configures the valid lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.

DHCPv6 Client Parameter Configuration

Use the following example to configure the DHCPv6 client parameters to support DHCPv6-based address assignment:

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-client
        server-ipv6-address <ipv6_addr> port <port> priority <priority>
        max-retransmissions <max_number>
        server-dead-time <dead_time>
        server-resurrect-time <revive_time>
      end
    end
```

Notes:

- DHCPv client configuration requires an IPv6 address, port, and priority. The port is used for communicating with the DHCPv6 server. If not specified, default port 547 is used. The Priority parameter defines the priority in which servers should be tried out.
- **max-retransmissions** configures the max retransmission that DHCPV6-CLIENT will make towards DHCPV6-SERVER. Default is 20.
- **server-dead-time**: PDN DHCPV6-SERVER is considered to be dead if it does not respond after given tries from client. Default is 5.

- **server-resurrect-time:** PDN DHCPv6-SERVER is considered alive after it has been dead for given seconds. Default is 20.

DHCPv6 Profile Configuration

Use the following example to configure the DHCPv6 profile:

configure

```

context <dest_ctxt_name>
  dhcp-server-profile <server_profile>
    enable rapid-commit-dhcpv6
    process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority <priority>
    dhcpv6-server-preference <pref_value>
    enable dhcpv6-server-unicast
    enable dhcpv6-server-reconf
    exit
  dhcp-client-profile <client_profile>
    dhcpv6-client-unicast
    client-identifier { IMSI | MSISDN }
    enable rapid-commit-dhcpv6
    enable dhcp-message-spray
    request dhcp-option dns-address
    request dhcp-option netbios-server-address
    request dhcp-option sip-server-address
  end

```

Notes:

- **dhcp-server-profile** command allows to create a server profile and then enter the DHCP Server Profile configuration mode.
- **enable rapid-commit-dhcpv6** command enables rapid commit on the DHCPv6 server. By default it is disabled. This is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the ue.
- **process dhcp-option-from** command configures in what order should the configuration options be processed for a given client request. For a given client configuration, values can be obtained from either AAA, PDN-DHCP-SERVER, or LOCAL. By default, AAA is preferred over PDN-DHCP which is preferred over LOCAL configuration.
- **dhcpv6-server-preference:** According to RFC-3315, DHCPv6-CLIENT should wait for a specified amount of time before considering responses to its queries from DHCPv6-SERVERS. If a server responds with a preference value of 255, DHCPv6-CLIENT need not wait any longer. Default value is 0 and it may have any integer between 0 and 255.
- **enable dhcpv6-server-unicast** command enables server-unicast option for DHCPv6. By default, it is disabled.
- **enable dhcpv6-server-reconf** command configures support for reconfiguration messages from the server. By default, it is disabled.
- **dhcp-client-profile** command allows to create a client profile and then enter the DHCP Client Profile configuration mode.
- **dhcpv6-client-unicast** command Enables client to send messages on unicast address towards the server.

- **client identifier** command configures the client-identifier which is sent to the external dhcp server. By default, IMSI is sent. Another available option is MSISDN.
- **enable rapid-commit-dhcpv6** command configures the rapid commit for the client. By default rapid-commit option is enabled for DHCPv6.
- **enable dhcp-message-spray** command enables dhcp-client to spray a dhcp messages to all configured dhcp servers in the PDN. By default this is disabled. With Rapid-Commit, there can only be one server to which this can be sent.
- **request dhcp-option** command configures DHCP options which can be requested by the dhcp-client. It supports the following options:
 - dns-address
 - netbios-server-address
 - sip-server-address

Associate DHCPv6 Configuration

Use the following example to associate the DHCPv6 profile with an APN:

```
configure
    context <dest_ctxt_name>
        apn <apn_name>
            dhcpv6 service-name <dhcpv6_svc_name> server-profile <server_profile>
        client-profile <client_profile>
            dhcpv6 ip-address-pool-name <dhcpv6_ip_pool>
            dhcpv6 context-name <dest_ctxt>
        exit
```

Notes:

- **dhcpv6 ip-address-pool-name** command is optional. In case pool name is not specified, it searches across all the configured static pools.

DHCPv6 Service Configuration Verification

Step 1

Verify that your DHCPv6 servers configured properly by entering the following command in Exec Mode:

show dhcpv6-service all

This command produces an output similar to that displayed below where DHCPv6service name is *dhcpv6-service*:

```
Service name:          dhcpv6-service
Context:               A
Bind Address:         2092::192:90:92:40
Bind :                Done
Service Status:       Started
Server Dead Time:     120 (secs)
Server Dead consecutive Failure:5
Server Select Algorithm: First Server
Server Renew Time:    400 (secs)
Server Rebind Time:   500 (secs)
Server Preferred Life Time: 600 (secs)
Server Valid Life Time: 700 (secs)
```

```

Max Retransmissions:          3 (secs)
Server Dead Tries:           4 (secs)
Server Resurrect Time:       10 (secs)
ipv6_nd_flag:                O_FLAG
DHCPv6 Servers configured:
    Address:                  2092::192:90:92:40 Priority: 1
enabled

```

- Step 2** Verify the DHCPv6 service status by entering the following command in Exec Mode:
show dhcpv6 status servicedhcpv6_service_name

DNS Configuration for IPv4v6 PDP Context

The system can be configured to provide DNS support for IPv4v6 PDP context.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and APN as described in *APN Configuration* section of this chapter.

To configure the DNS support for IPv4v6 PDP context:

-
- Step 1** Configure the list of domain name servers with IPv4/IPv6 address in context configuration mode by applying the example configuration in the *Creating IPv4 and IPv6 DNS List* section.
- Step 2** Configure the IPv4 primary and secondary domain name server in APN configuration mode by applying the example configuration in the *Configuring IPv4 DNS* section.
- Step 3** Configure the IPv6 primary and secondary domain name server in APN configuration mode by applying the example configuration in the *Configuring IPv6 DNS* section.
- Step 4** Verify your DNS configuration by following the steps in the *APN Configuration Verification*.
- Step 5** Save your configuration as described in the *Verifying and Saving Your Configuration*.
-

Creating IPv4/IPv6 DNS List

Use the following example to create the domain name server list in context configuration mode:

```

configure
    context <src_ctxt_name>
        ip name-server <ip_address secondary_ip_address>
    end

```

Notes:

- <ip_address> is primary IP address of the domain name server having IPv4/IPv6 address.
- <secondary_ip_address> is the secondary IP address of the domain name server having IPv4/IPv6 address.
- Multiple DNS can be configured by entering **ip name-server** command multiple times.

Configuring IPv4 DNS

Use the following example to configure the IPv4 DNS support in IPv4v6 PDP context:

```
configure
  context <src_ctxt_name>
    apn <apn_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
    end
```

Notes:

- <ipv4_address> is the IP address of the domain name server configured as DNS list in context configuration mode.

Configuring IPv6 DNS

Use the following example to configure the IPv6 DNS support in IPv4v6 PDP context:

```
configure
  context <src_ctxt_name>
    apn <apn_name>
      ipv6 dns primary <ipv6_address>
      ipv6 dns secondary <ipv6_address>
    end
```

Notes:

- <ipv6_address> is the IP address of the domain name server configured as DNS list in context configuration mode.

IP Address Pool Configuration on the System

Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured.

IP addresses can be dynamically assigned from a single pool/a group of IP pools/a group of IP pool groups. The addresses/IP pools/ IP pool groups are placed into a queue in each pool or pool group. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

On initiation of a session, a request of IP address from IP pool is sent and system assigns an IP address out of "available" IP address(es) in the pool. This assigned IP address is set to "allocated" state and cannot be used for any other session during this state. As soon as the session is cleared the state of "allocated" IP address is changed to "released" and is ready for allocation to any other subscriber session. If a "hold" timer is set for assigned/released IP address(es), it will go into the "hold" state and remain there till the timer expires. As soon as "hold timer" expires its state is changed from "hold" to "released" state and it will be available for reallocation. The "available" IPs include "free" and "released" IP addresses.

Free IPs are used first depending on which subscriber is connecting. Normally same IP is given to a subscriber. So if a subscriber is connecting again, instead of using a free IP, GGSN allocates the IP which was given to him previously. This IP will be from the released state. For GGSN, Username and IMSI are used as key for generating subscriber ID used by VPN while allocating IP from the IP pool. Therefore if the subscriber ID matches to any of the previous ones for IPs in released state, that IP is re-allocated to that subscriber, otherwise a new IP is allocated.

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

**Important**

Setting different priorities on each individual pool can cause addresses in some pools to be used more frequently.

**Important**

This section provides the minimum instruction set for configuring local IP address pools on the system. For more information on commands that configure additional parameters and options, refer ip pool command section in *Context Configuration Mode Commands* chapter of *Command Line Interface Reference*.

**Caution**

From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.

**Caution**

In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the IP pool:

-
- Step 1** Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.
 - Step 2** Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.
 - Step 3** Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.
 - Step 4** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.
-

IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

```
configure
  context <dest_ctxt_name>
    ip pool <pool_name> <ip_address/mask> [{private|public}[priority]] | static
  end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer `ipv6 pool` command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IPv6 Pool Creation

Use the following example to create the IPv6 address pool:

```
configure
  context <dest_ctxt_name>
    ipv6 pool <pool_name> 6to4 local-endpoint <ip_address>[private][public][shared][static]
  end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer `ipv6 pool` command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IP Pool Configuration Verification

Step 1

Verify that your IPv4 address pool configured properly by entering the following command in Exec Mode:

show ip pool

The output from this command should look similar to the sample shown below. In this example all IP pools were configured in the *ispl* context.

```
context : ispl:
+-----Type:          (P) - Public          (R) - Private
|                      (S) - Static          (E) - Resource
|
|+-----State:        (G) - Good            (D) - Pending Delete          (R) -Resizing
||
||+-----Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+--Busyout: (B) - Busyout configured
|||||
|||||
vvvvvv Pool Name      Start Address      Mask/End Address      Used      Avail
-----
PG00    ipsec         12.12.12.0            255.255.255.0         0          254
RG00    pool3         30.30.0.0             255.255.0.0           0
65534
SG00    pool2         20.20.0.0             255.255.0.0           10
65524
PG00    pool1         10.10.0.0             255.255.0.0           0
65534
SG00    vpnpool      192.168.1.250         192.168.1.254         0          5
Total Pool Count: 5
```

Step 2

Verify that your IPv6 address pools configured properly by entering the following command in Exec Mode:

show ipv6 pools

The output from this command should look similar to the sample shown above except IPv6 addresses.

Gn-Gp Handoff Support Configuration

This section describes all about the configurations that are required to enable the handoff between the 3GPP 2G/3G SGSN and P-GW over Gn-Gp interfaces.



Important

This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Gn-Gp handoff on GGSN node:

-
- | | |
|---------------|--|
| Step 1 | Create and configure the GTP-U service by applying the example configuration in the <i>GTP-U Service Configuration</i> section. |
| Step 2 | Modify GGSN service to facilitate the handoff between SGSN/GGSN and P-GW by applying the example configuration in the <i>Modifying GGSN Configuration for Gn-Gp Handoff</i> section. |
| Step 3 | Modify APN configuration to the "subscribed" selection mode by applying the example configuration in <i>APN Configuration for Gn-Gp Handoff</i> section. |
| Step 4 | Verify your handoff configuration by following the steps in the <i>Gn-Gp Configuration Verification</i> section. |
| Step 5 | Save your configuration as described in the <i>Verifying and Saving Your Configuration</i> chapter. |
-

GTP-U Service Configuration

Use the following example to configure the GTP-U service:

```
configure
  context <ctxt_name> -noconfirm
    gtpu-service <gtpu_svc_name>
      bind ipv4-address <ip_address>
      echo-interval <time_interval>
    end
```

Notes:

- <ctxt_name> is name of the context which contains GTPU service on system.
- <time_interval> is the time interval in seconds at which GPRS Tunneling Protocol (GTP) v1-U Echo packets are sent.
- <ip_address> is the IP address of IPv4 or IPv6 type to which the GTP-U service will be binded.

Modifying GGSN Configuration for Gn-Gp Handoff

Use the following example to create/modify the GGSN config for this feature.

```
configure
  context <ctxt_name>
    ggsn-service <ggsn_svc_name>

      associate gtpu-service <gtpu_svc_name>
      associate pgw-service <pgw_svc_name>
      bind address <ip_address>
    end
```

Notes:

- <ggsn_svc_name> is name of the existing GGSN service.
- <gtpu_svc_name> is name of the existing GTP-U service created in *GTP-U Service Configuration* example.

- `<pgw_svc_name>` is the existing P-GW service name.
- `<ip_address>` is the same IP address to which GTP-U service is binded in *GTP-U Service Configuration* example.
- `<ctxt_name>` is the name of the context which contains the GGSN service.

APN Configuration for Gn-Gp Handoff

Use the following example to modify the APN configuration for the smooth handover support between SGSN/GGSN and P-GW:

```
configure
context <ctxt_name>
  apn <apn_name>
  selection-mode subscribed
  ip context-name <ctxt_name>
  pdp-type <ipv4 | ipv6>
end
```

Notes:

- Make sure that the APN Selection mode parameters setting is set to "subscribed", which is also the default mode.

Gn-Gp Configuration Verification

Verify that all the configurations made in a specific context under Context Configuration mode are in place and the P-GW service and GTP-U services have been associated to the GGSN service by entering the following command in Exec mode:

show ggsn-service name ggsn

The output from this command should look similar to the sample shown below. In this example context name *A* was created in Exec mode, GGSN service *ggsn* was created in GGSN Service Configuration mode, PGW service named *pgw* was an already configured service and GTP-U service named *gtpu* was configured in the GTPU Service Configuration mode:

```
Service name:                ggsn
context:                     A
Associated PGW svc:          pgw
Associated GTPU svc:         gtpu
.
.
Bind:                        Done
Local IP Address:           120.56.45.12      Local IP Port:      2123
...
...
Echo Interval:              60 (secs)
.
.
.
```

FA Services Configuration

FA services are configured within contexts and allow the system to function as an FA in the 3G wireless data network.



Important

This section provides the minimum instruction set for configuring an FA service that allows the system to process data sessions. Commands that configure additional FA service properties are provided in the Command Line Interface Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the FA service:

- Step 1** Create the FA service in the system context created to facilitate FA service by applying the example configuration in the *FA Service Creation* section.
- Step 2** Bind the configured FA service to a local IP address interface with UDP port and specify the maximum number of subscribers that can access this service for the Pi interfaces' IP socket by applying the example configuration in the *IP Interface and UDP Port Binding for Pi Interface* section.
- Step 3** Configure the security parameter index (SPI) between FA service and HA by applying the example configuration in the *Security Parameter Index (SPI) Configuration* section.
- Step 4** Specify the FA agent advertisement related parameters like lifetime, number of advertisements, and registration lifetime by applying the example configuration in the *FA Agent Advertisement Parameter Configuration* section.
- Step 5** Configure the number of registration per subscriber, authentication procedure, and registration timeout parameters for this FA service by applying the example configuration in the *Subscriber Registration, Authentication and Timeout Parameter Configuration* section.
- Step 6** Optional. Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages by applying the example configuration in the *Revocation Message Configuration* section.
- Step 7** Verify your FA service configuration by following the steps in the *FA Service Configuration Verification* section.
- Step 8** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

FA Service Creation

Use the following example to create the FA service:



Important

A maximum of 256 services (regardless of type) can be configured per system.

```
configure
context <fa_ctxt_name> -noconfirm
```

```
fa-service <fa_svc_name> -noconfirm]
end
```

Notes:

- <fa_ctxt_name> is name of the context to use for FA service configuraiton. Generally FA should be configured within a destination context.
- <fa_svc_name> is name of the FA service where other parameters have to configure for FA functionality.

IP Interface and UDP Port Binding for Pi Interface

Use the following example to bind the FA service to an local IP interface and specify the maximum number of subscribers that can access this service. Binding an interface to the FA service causes the interface to take on the characteristics of a Pi interface.

configure

```
context <fa_ctxt_name>
fa-service <fa_svc_name>
bind address <fa_ip_address> max-subscribers <max_subs>
ip local-port <udp_port_num>
end
```

Notes:

- <fa_svc_name> is name of the FA service which is created to configure FA functionality.
- <fa_ip_address> is the local IP address in IPv4/IPv6 notation for providing Pi interface characteristics.
- <max_subs> is the maximum number of subscribers that can access this service on this interface. This can be configured to any integer value from 0 to 500,000. The default is 500,000.



Important

The maximum number of subscribers supported is dependant on the session capacity license installed and the number of active PACs/PSCs installed in the system. For more information on session capacity license, refer to the Software Management Operations chapter of the System Administration Guide.

- <udp_port_num> is the UDP port number from 1 through 65535 to be used for Pi interface. Default port number is 434.
- For more information on commands/keywords that configure additional parameters and options, refer *FA Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Security Parameter Index (SPI) Configuration

Use the following example to configure the security parameter index (SPI) between FA service and HA:



Important

A maximum of 2048 FA-HA SPIs can be configured for a single FA service.

configure

```
context <fa_ctxt_name>
```

```

fa-service <fa_svc_name>
  fa-ha-spi remote-address <ha_ip_address> spi-number <spi_num> {encrypted secret
<enc_secret_key> | secret <secret_key>} [description <desc_string>]
end

```

Notes:

- <fa_svc_name> is name of the FA service which is created to configure FA functionality.
- <ha_ip_address> is the IP address in IPv4/IPv6 notation of HA to which this FA service will interact.
- <spi_num> specifies the SPI number which indicates a security context between the FA and the HA in accordance with RFC 2002 and can be configured to any integer value from 256 through 4294967295.
- <enc_secret_key> specifies the encrypted shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.



Important

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

- <secret_key> specifies the secret shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
- <desc_string> is the description for this SPI and must be from 1 to 31 alpha and/or numeric characters.
- For more information on commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

FA Agent Advertisement Parameter Configuration

Use the following example to configure the agent advertisement parameters for this FA service:

configure

```

context <fa_ctxt_name>
  fa-service <fa_svc_name>
    advertise adv-lifetime <adv_dur>
    advertise num-adv-sent <adv_num>
    advertise reg-lifetime <reg_dur>
  end
end

```

Notes:

- <fa_svc_name> is name of the FA service which is created to configure FA functionality.
- <adv_dur> is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default is 9000.
- <adv_num> is the number of unanswered agent advertisements that the FA service allows during call setup before it rejects the session. It can be any integer value from 1 to 65535. The default is 3.
- <reg_dur> specify the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. It is measured in seconds and can be configured to any integer value from 1 to 65534. The default is 600.

Subscriber Registration, Authentication and Timeout Parameter Configuration

Use the following example to configure the number of subscriber registration, authentication procedure and registration timeout parameters for this FA service:

configure

```

    context <fa_ctxt_name>
      fa-service <fa_svc_name>
        multiple-reg <reg_num>
        reg-timeout <timeout_dur>
        authentication mn-aaa {always | ignore-after-handoff | init-reg | init-reg-except-handoff
| renew-and-dereg-noauth | renew-reg-noauth} [optimize-retries]
      end

```

Notes:

- <fa_svc_name> is name of the FA service which is created to configure FA functionality.
- <reg_num> is the number of simultaneous Mobile IP sessions that are to be supported for a single subscriber. It can be configured to any integer value from 1 to 3. The default value is 1.



Important

The system supports multiple Mobile IP sessions per subscriber only if the subscriber's mobile node has a static IP address. The system only allows a single Mobile IP session for mobile nodes that receive a dynamically assigned home IP address.



Important

In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

- <timeout_dur> is the maximum amount of time that the FA service waits for a Registration Rely message from the HA. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default value is 45.
- For more information on authentication mn-aaa commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

Revocation Message Configuration

Use the following example to configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:

configure

```

    context <fa_ctxt_name>
      fa-service <fa_svc_name>
        revocation negotiate-i-bit
      end

```

Notes:

- By default the system will not send the I-bit in the revocation message.

FA Service Configuration Verification

Step 1 Verify that your FA service is configured properly by entering the following command in Exec Mode:

show fa-service all

The output from this command should look similar to the sample shown below. In this example an FA service named `fa1` was configured in the `isp1` context.

```
Service name:          fa1
Context:              isp1
Bind:                 Done
500000                                Max Subscribers:
Local IP Address: 195.20.20.3          Local IP Port          434
Lifetime:             00h10m00s        Registration Timeout: 45 (secs)
Advt Lifetime         02h30m00s        Advt Interval:         5000 (msecs)

Num Advt:              5
Advt Prefix Length Extn: NO
Reverse Tunnel:        Enabled          GRE Encapsulation:      Enabled
SPI(s):
FAHA: Remote Addr: 195.30.30.3/32
Hash Algorithm:        HMAC_MD5        SPI Num:              1000
Replay Protection: Timestamp            Timestamp Tolerance: 60
IPSEC Crypto Map(s):
Peer HA Addr:          195.30.30.2
Crypto Map:            test
Registration Revocation: Enabled        Reg-Revocation I bit:   Enabled
Reg-Revocation Max Retries: 3            Reg-Revocation Timeout: 3 (secs)
Reg-Rev on InternalFailure: Enabled
```

Step 2 Verify configuration for errors in FA service by entering the following command in Exec Mode:

show configuration errors section fa-service verbose

Common Gateway Access Support Configuration

This section describes some advance feature configuration to support multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS for international roaming with the same IP addressing behavior and access to 3GPP AAA for subscriber authorization. Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

This configuration combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow subscribers to have the same user experience, independent of the access technology available.



Important

This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the S6b and other advance features:

-
- | | |
|---------------|--|
| Step 1 | Configure Diameter endpoint by applying the example configuration in the <i>Diameter Endpoint Configuration</i> section. |
| Step 2 | Create or modify AAA group by applying the example configuration in the <i>AAA Group Configuration</i> section. |
| Step 3 | Modify GGSN service to allow authorization with HSS by applying the example configuration in the <i>Authorization over S6b Configuration</i> section. |
| Step 4 | <i>Optional.</i> Create and associate DNS client parameters by applying the example configuration in the <i>DNS Client Configuration</i> section. |
| Step 5 | <i>Optional.</i> Modify GGSN service to accept duplicate calls when received with same IP address by applying the example configuration in the <i>Duplicate Call Accept Configuration</i> section. |
| Step 6 | Verify your S6b configuration by following the steps in the <i>Common Gateway Access Support Configuration Verification</i> section. |
| Step 7 | Save your configuration as described in the <i>Verifying and Saving Your Configuration</i> chapter. |
-

Diameter End-Point Configuration

Use the following example to define the diameter accounting end-point and associate a diameter accounting dictionary for this feature:

```
configure
  context <ctxt_name>
    diameter endpoint <endpoint_name>
      origin host <diameter_host_name> address <ip_address>
      peer <peer_name> realm <peer_realm_name>
    address <ip_address>
    port <port_number>
  end
```

AAA Group Configuration

Use the following example create/modify the AAA group for this feature.

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
      diameter authentication endpoint <s6b_endpoint_name>
      diameter authentication server <server_name> priority <priority>
    end
```

Notes:

- <s6b_endpoint_name> is name of the existing Diameter endpoint.

Authorization over S6b Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:

```
configure
  context <ggsn_ctxt_name>
    ggsn-service <ggsn_svc_name>
      plmn-unlisted-sgsn home
      authorize-with-hss
      fqdn host <host_name> realm <realm_name>
    end
```

Notes:

- <ggsn_svc_name> is name of the GGSN service which is already created on the system.

DNS Client Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:

```
configure
  context <ggsn_ctxt_name>
    ip domain-lookup
    ip name-servers <ip_address/mask>
    dns-client <dns_name>
      bind address <ip_address>
      resolver retransmission-interval <duration>
      resolver number-of-retries <retrie>
      cache ttl positive <ttl_value>
    exit
    ggsn-service <ggsn_svc_name>
      default dns-client context
    end
```

Notes:

- <ggsn_svc_name> is name of the GGSN service which is already created on the system.

Duplicate Call Accept Configuration

Use the following example to configure GGSN service to accept the duplicate session calls with request for same IP address:

```
configure
  context <ggsn_ctxt_name>
    ggsn-service <ggsn_svc_name>
      newcall duplicate-subscriber-requested-address accept
    end
```

Notes:

- <ggsn_svc_name> is name of the GGSN service which is already created on the system.

Common Gateway Access Support Configuration Verification

Verify that your common gateway access support is configured properly by entering the following command in Exec Mode:

show ggsn-service all

The output from this command should look similar to the sample shown below. In this example GGSN service named *GGSN1* was configured in the *vpn1* context.

```
Service name:                ggsn1
Context:                     cn1
Associated PGW svc:          None
Associated GTPU svc:         None
Accounting Context Name:cn1
dns-client Context Name:cn1
Authorize:                   hss
Fqdn-name:                   xyz.abcstarent.networks.com
Bind:                        Not Done
Local IP Address:            0.0.0.0
Self PLMN:                   Not defined
Retransmission Timeout: 5 (secs)
Local IP Port:                2123
```

Rf Interface Configuration for Offline Charging

This section describes the step-by-step procedure for the configurations that are required to setup the Rf interface on GGSN to support offline charging.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Rf interface on GGSN node:

- Step 1** Create and configure the accounting policy by applying the example configuration in the *Accounting Policy Configuration* section.
- Step 2** Configure a AAA group to associate the diameter accounting dictionary with the by applying the example configuration in the *AAA Group Configuration* section.
- Step 3** Configuring an APN to associate the accounting policy by applying the example configuration in *APN Configuration for Rf Interface* section.
- Step 4** Verify your Rf interface configuration by following the steps in the *Rf Interface Configuration Verification*
- Step 5** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Accounting Policy Configuration

Use the following example to configure the accounting policy for this feature:

```
configure
  context <ctxt_name>
    policy accounting <policy_name>
      operator-string <ip_address>
      accounting-level [ sdf | flow ]
      cc profile [ 2 | 4 | 6 | 8 ] [ buckets | interval | sdf-interval | sdf-volume | serving nodes | tariff
| volume ]
    end
```

Diameter End-Point Configuration

Use the following example to define the diameter accounting end-point and associate a diameter accounting dictionary for this feature:

```
configure
  context <ctxt_name>
    diameter endpoint <endpoint_name>
      origin host <diameter_host_name> address <ip_address>
      peer <peer_name> realm <peer_realm_name>
    address <ip_address>
    port <port_number>
  end
```

AAA Group Configuration

Use the following example to create/modify the AAA group for this feature:

```
configure
  context <ctxt_name>
    aaa group <group_name>
      diameter accounting endpoint <endpoint_name>
      diameter accounting dictionary [ aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3
| aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 ]
      diameter accounting server <diameter_hostname> priority <number>
    end
```

APN Configuration for Rf Interface

Use the following example create/modify the APN configuration for this feature:

```
configure
  context <ctxt_name>
    apn <apn_name>
      associate accounting-policy <policy_name>
    end
```

Rf Interface Configuration Verification

Verify that your Rf interface configuration for offline charging support is configured properly by entering the following command in Exec Mode:

show configuration context *ctxt_name*

The output from this command should look similar to the sample shown below. In this example accounting policy named *test_policy* was configured in the *rf_context* context.

```
config
  context rf_context
    subscriber default
    exit
    apn apn
      associate accounting-policy test_policy
    exit
    aaa group default
    exit
    aaa group rf_aaa
      diameter accounting dictionary aaa-custom6
      diameter accounting endpoint rf_endpoint
      diameter accounting server rf_server priority 2
    exit
    gtp group default
    exit
    policy accounting test_policy
      accounting-level flow
      operator-string Rf_string
      cc profile 2 buckets 5
    exit
    diameter endpoint rf_endpoint
      origin host rf_diameter address 1.2.3.4
      peer ak realm ak_realm address 2.3.4.5 port 52
    exit
    ip igmp profile default
    exit
  exit
end
```

Configuring RFL Bypass Feature

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature. The RLF feature allows the operator to control the bypassing of some messages being throttled.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.

Configuring the Throttling Override Policy Mode

The following configuration helps to create a GTP-C Throttling Override Policy and to enter GTP-C Throttling Override Policy mode.

configure

throttling-override-policy *throttling-override-policy_name*

Notes:

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-throttling-override-policy)
```

Configuring the RLF Bypass Feature

The following configuration configures message types which can bypass the rate limiting function.

```
configure
  throttling-override-policy throttling-override-policy_name
    [ default | no ] egress bypass-rlf ggsn msg-type { dpc | ipca | nrupe | emergency-call | arp { 1 | 2 |
3 }+ | apn-names <apn-name1> <apn-name2> <apn-name3> }
  end
```

Notes:

- If an empty throttling-override-policy is created, then the default values for all the configurables are zeros/disabled.
- If no throttling-override-policy is associated, then **show service configuration** for GGSN will show it as "n/a".
- Maximum number of throttling-override-policy that can be added are 1024. This limit is the same as max RLF templates.

Example

The following command configures Delete PDP message type at the GGSN node to bypass throttling.

```
egress bypass-rlf ggsn msg-type dpc
```



GGSN Configuration Example

This chapter provides information for configuring the system to function as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.



Important

This chapter does not discuss the configuration of the local context. Information about the local context can be found in the *Command Line Interface Overview* chapter of the *System Administration Guide* and the *Command Line Interface Reference*.

The most simple configuration that can be implemented on the system to support GGSN functionality requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

The source context facilitates the following:

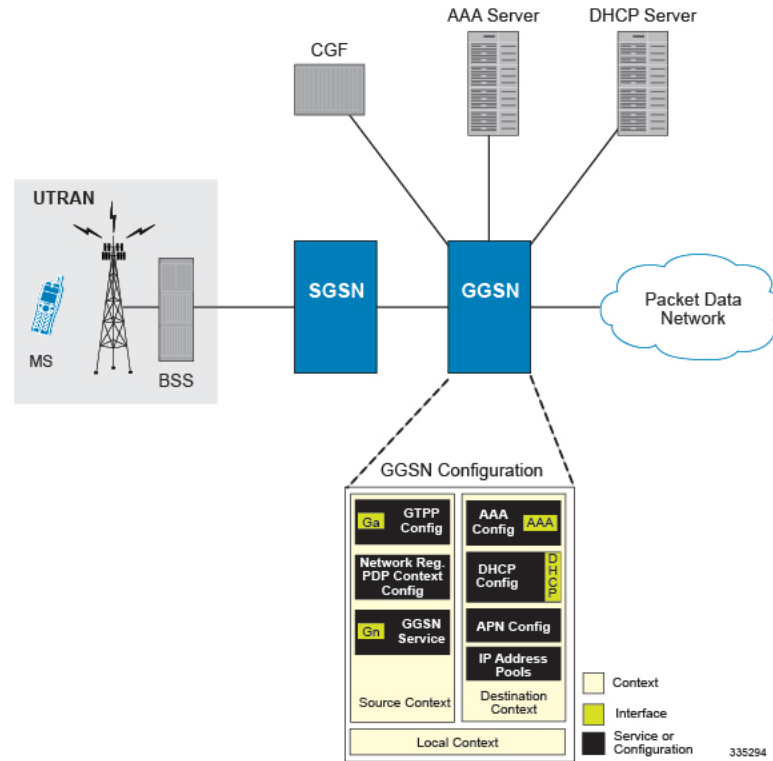
- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

- Access Point Name (APN) configuration
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts.

Figure 18: GGSN Support Using a Single Source and Destination Context



This chapter contains the following sections:

- [Information Required, page 122](#)
- [How This Configuration Works, page 132](#)

Information Required

The following sections describe the minimum amount of information required to configure and make the GGSN operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the GGSN in the network. Information on these parameters can be found in the appropriate sections of the Command Line Reference.

Source Context Configuration

Table 1: Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number can be any integer value from 1 to 65535. The default value is 2123.

Required Information	Description
Public Land Mobile Network (PLMN) Identifiers	Mobile Country Code (MCC): The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.

Required Information	Description
GGSN charging characteristics (CC) (optional)	<p>Behavior Bits: If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p> <p>Profile Index: If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). • Prepaid accounting can be disabled for a specified profile index. <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15</p>
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)

Required Information	Description
Ga Interface Configuration	
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	IP address: The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	Priority: If more than one CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages: The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.

Required Information	Description
GCDR optional fields	<p>The following optional fields can be specified/configured in CDRs generated by the GGSN:</p> <ul style="list-style-type: none"> • diagnostics • duration-ms (the time specified in the mandatory Duration field is reported in milliseconds) • local-record-sequence-number • plmn-id
Network Requested PDP Context Support Configuration (optional)	
Activation Requirements	<p>IP address: The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.</p>
	<p>Destination context name: The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.</p>
	<p>International Mobile Subscriber Identity (IMSI): The IMSI of the mobile station.</p>
	<p>APN: The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.</p>
GSN-map node	<p>Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.</p>

Destination Context Configuration

Table 2: Required Information for Destination Context Configuration

Required Information	Description
Destination context name	<p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.</p> <p>Important For this configuration, the destination context name should not match the domain name of a specific APN.</p>
APN Configuration	

Required Information	Description
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. Important The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. Important The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.
IP address allocation method	Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods: <ul style="list-style-type: none"> • Dynamic: Address can be dynamically assigned from one of the sources. <ul style="list-style-type: none"> • Dynamic Host Control Protocol (DHCP) server: The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS. • Local address pools: The system can be configured with local address pools. • Static: MS IP addresses can be permanently assigned. <p>By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.</p>
IP address pool name	If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.

Required Information	Description
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
PDP type	The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default. For IPv6 PDP configuration, at least one IPv6 interface needs to be configured in the destination context.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: <ul style="list-style-type: none"> • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)
DHCP Interface Configuration (optional)	
DHCP interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Gateway IP address	Used when configuring static routes from the DHCP interface(s) to a specific network.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	

Required Information	Description
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured. Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.
Lease Duration	Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. <ul style="list-style-type: none"> • Minimum Lease Time: Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds. • Maximum Lease Time: Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	

Required Information	Description
RADIUS Authentication server	IP Address: Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	IP Address: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
PDN Interface Configuration	
PDN interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.

Required Information	Description
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	This is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.
Pool addresses, subnet mask and type	The pool can consist of either of the following: <ul style="list-style-type: none"> • An entire subnet configured using the initial address and the subnet mask • A range of addresses configured using the first and last IP addresses in the range <p>The pool can be configured as public, private, or static. Public pools can also be assigned a priority.</p>

How This Configuration Works

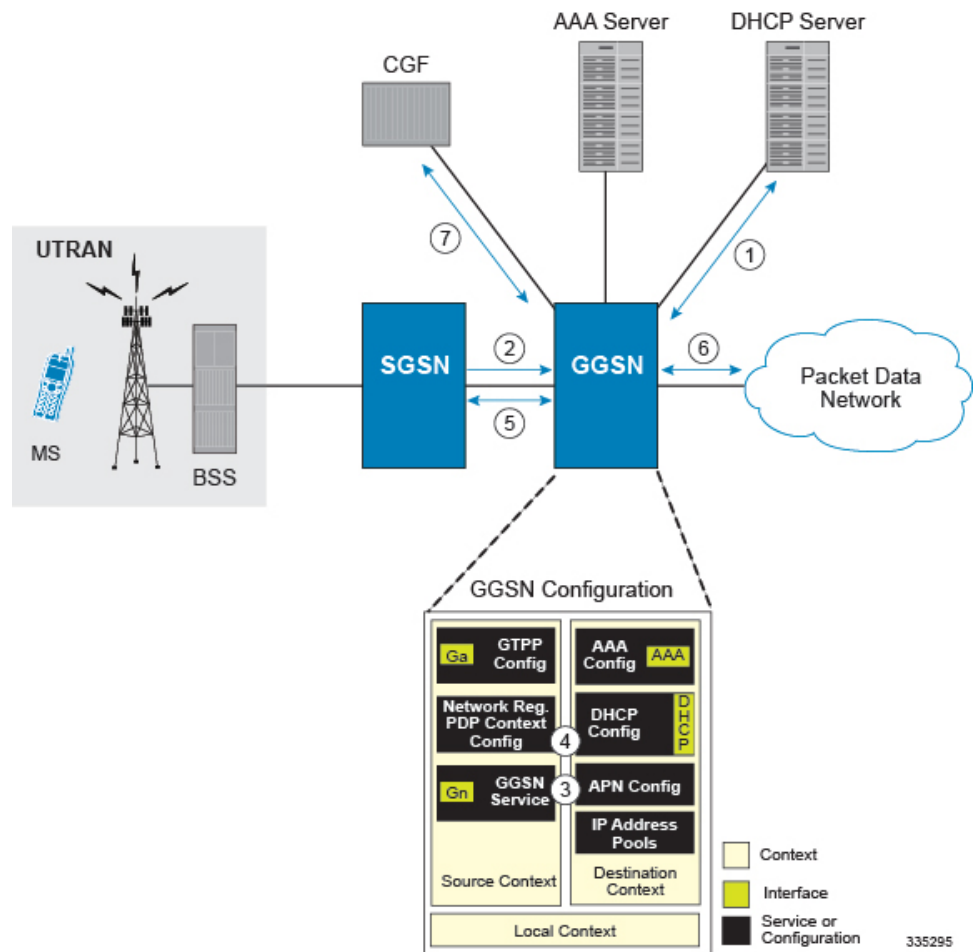
This section provides a description of how the information detailed in the previous sections of this chapter are used in the processing of the following types of subscriber sessions:

- [Transparent IP PDP Context Processing, on page 133](#)
- [Non-transparent IP PDP Context Processing, on page 134](#)
- [PPP PDP Context Processing, on page 135](#)
- [Network-requested PDP Context Processing, on page 136](#)

Transparent IP PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a transparent IP PDP context.

Figure 19: Transparent IP PDP Context Call Processing



- 1 If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
- 2 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 3 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
- 4 If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.

- 5 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 6 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
- 7 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Non-transparent IP PDP Context Processing

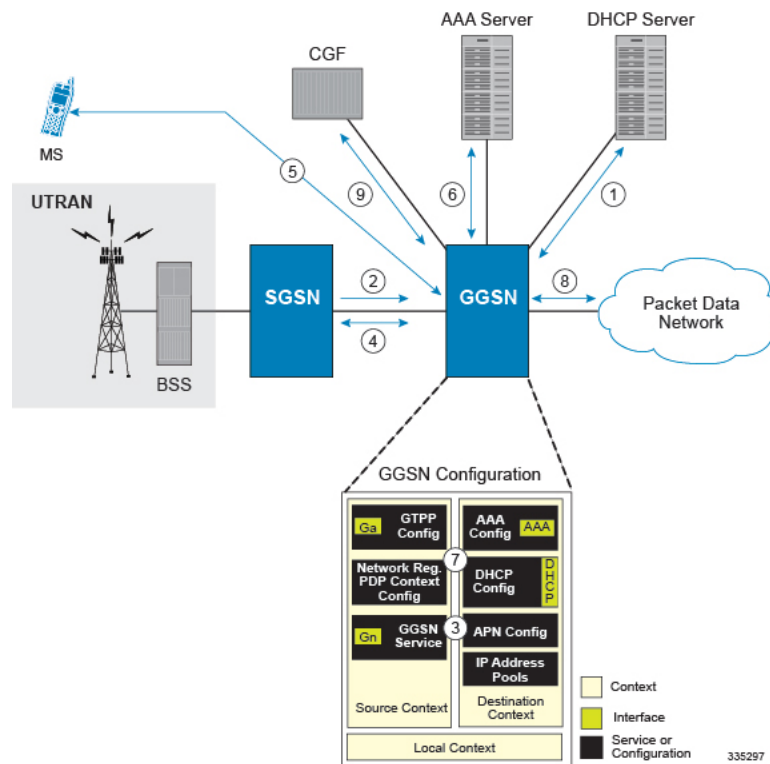
The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a non-transparent IP PDP context.

- 1 If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
- 2 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 3 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
- 4 If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
- 5 If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
- 6 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 7 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
- 8 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

PPP PDP Context Processing

The following figure and the following text describe how this configuration with a single source and destination context would be used by the system to process a PPP PDP context.

Figure 21: PPP PDP Context Call Processing

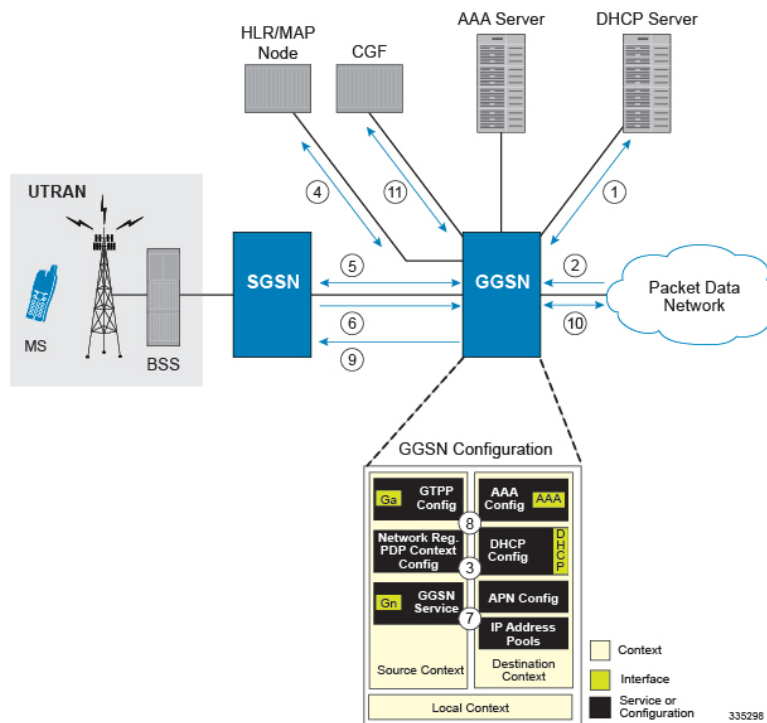


- 1 If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
- 2 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 3 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
- 4 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 5 The MS and GGSN negotiate PPP.
- 6 The GGSN authenticates the subscriber as part of the PPP negotiation by communicating with a RADIUS server over the AAA interface.
- 7 Upon successful authentication, the GGSN assigns an IP address to the MS from one of those stored in its memory cache.
- 8 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
- 9 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Network-requested PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a network-requested PDP context.

Figure 22: Network-requested PDP Context Call Processing



- 1 If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
- 2 An IP packet data unit (PDU) is received by the GGSN from the PDN.
- 3 The GGSN determines if it is configured to support network-initiated sessions. If so, it begins the Network-Requested PDP Context Activation procedure, otherwise it discards the packet.
- 4 The GGSN determines if the MS is reachable by communicating with the HLR through a MAP node over one of the Gn interfaces.
- 5 The GGSN works with the SGSN to activate the MS.
- 6 Once activated, the MS initiates a PDP context resulting in the sending of a Create PDP Context Request message from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 7 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
- 8 If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
- 9 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 10 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.

- 11 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.



Mobile IP Configuration Examples

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.



Important

This chapter does not discuss the configuration of the local context. Information about the local context can be found in *Command Line Reference*.



Important

When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations* appendix.

- [Example 1: Mobile IP Support Using the System as a GGSN/FA, page 139](#)
- [Example 2: Mobile IP Support Using the System as an HA, page 152](#)
- [Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts, page 160](#)

Example 1: Mobile IP Support Using the System as a GGSN/FA

For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how the system performs the role of the GGSN/FA. Examples 2 and 3 provide information on using the system to provide HA functionality.

The system's GGSN/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure that follows.



Important

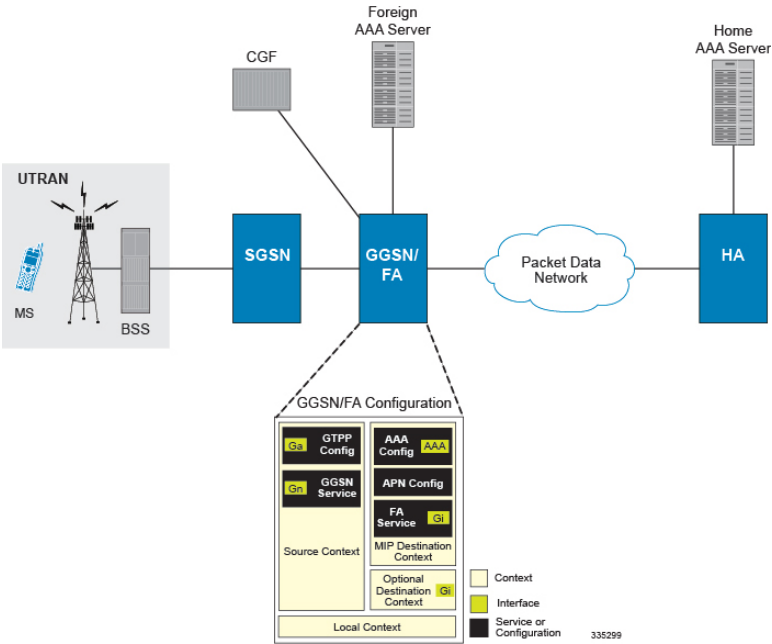
A fourth context that serves as a destination context must also be configured if Reverse Tunneling is disabled in the FA service configuration. Reverse Tunneling is enabled by default.

The source context will facilitate the GGSN service(s), and the Ga and Gn interfaces. The AAA context will be configured to provide foreign AAA functionality for subscriber PDP contexts and facilitate the AAA

interfaces. The MIP destination context will facilitate the FA service(s) and the Gi interface(s) from the GGSN/FA to the HA.

The optional destination context will allow the routing of data from the mobile node to the packet data network by facilitating a packet data network (PDN) interface. This context will be used only if reverse tunneling is disabled.

Figure 23: Mobile IP Support using the system as a GGSN/FA



Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 3: Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. Important The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide GGSN/FA functionality.
Gn Interface Configuration	

Required Information	Description
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	Mobile Country Code (MCC): The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.

Required Information	Description
SGSN information (optional)	<p>The GGSN can be configured with information about the SGSN(s) that it is to communicate with.</p> <p>This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.</p>
GGSN charging characteristics (CC) (optional)	<p>Behavior Bits: If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p> <p>Profile Index: If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15.</p>

Required Information	Description
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)
Ga Interface Configuration	
Ga interface name	<p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.</p>
IP address and subnet	<p>These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	<p>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the source context and are used to bind logical Ga interfaces.</p>
Gateway IP address	<p>Used when configuring static routes from the Ga interface(s) to a specific network.</p>
GTPP Configuration	
Charging gateway address	<p>The IP address of the system's GGSN interface.</p>

Required Information	Description
CGF server information	IP address: The IP address of the CGF server to which the GGSN will send accounting information .Multiple CGFs can be configured.
	Priority: If more than on CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages: The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: <ul style="list-style-type: none"> • diagnostics • duration-ms: the time specified in the mandatory Duration field is reported in milliseconds • local-record-sequence-number • plmn-id

AAA Context Configuration

Table 4: Required Information for AAA Context Configuration

Required Information	Description
AAA context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system. Important If a separate system is used to provide HA functionality, the AAA context name should match the name of the context in which the AAA functionality is configured on the HA machine.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.

Required Information	Description
Accounting mode	<p>Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP.</p> <p>Important The examples discussed in this chapter assumes GTPP is used.</p>
Authentication protocols used	<p>Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.</p>
APN charging characteristics (CC) (optional)	<p>Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers.</p> <p>By default the GGSN accepts the CC from the SGSN for all three scenarios.</p> <p>If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use.</p> <p>Important The profile index parameters are configured as part of the GGSN service.</p>
Domain Name Service (DNS) information (optional)	<p>If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.</p>
IP destination context name	<p>The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.</p>
Maximum number of PDP contexts	<p>The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.</p>
PDP type	<p>The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default.</p>
Verification selection mode	<p>The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods:</p> <ul style="list-style-type: none"> • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)

Required Information	Description
Mobile IP Configuration	<p>Home Agent IP Address: The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address.</p> <p>Parameters stored in individual profiles supersede parameters provided by the APN.</p> <p>Mobile IP Requirement: The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.</p>
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign RADIUS Server Configuration	

Required Information	Description
Foreign RADIUS Authentication server	<p>IP Address: Specifies the IP address of the Foreign RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers.</p> <p>Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>
Foreign RADIUS Accounting server (optional)	<p>IP Address: Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the foreign RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the foreign RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

Mobile IP Destination Context Configuration

Table 5: Required Information for Mobile IP Destination Context Configuration

Required Information	Description
Mobile IP Destination context name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system.</p> <p>Important For this configuration, the destination context name should not match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.</p>
Gi Interface Configuration	
Gi interface name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.</p>
IP address and subnet	<p>These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</p>
Physical port description(s)	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.</p>
Gateway IP address(es)	<p>Used when configuring static routes from the Gi interface(s) to a specific network.</p>
FA Service Configuration	
FA service name	<p>This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.</p>
UDP port number for Mobile IP traffic	<p>Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.</p>

Required Information	Description
Security Parameter Index (indices) Information	HA IP address: Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. NOTE: The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.

Required Information	Description
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.

Optional Destination Context Configuration

The following table lists the information required to configure the optional destination context. As discussed previously, this context is required if: 1) reverse tunneling is disabled in the FA service, or 2) if access control lists (ACLs) are used



Important

If ACLs are used, the destination context would only consist of the ACL configuration. Interface configuration would not be required.

Table 6: Required Information for Destination Context Configuration

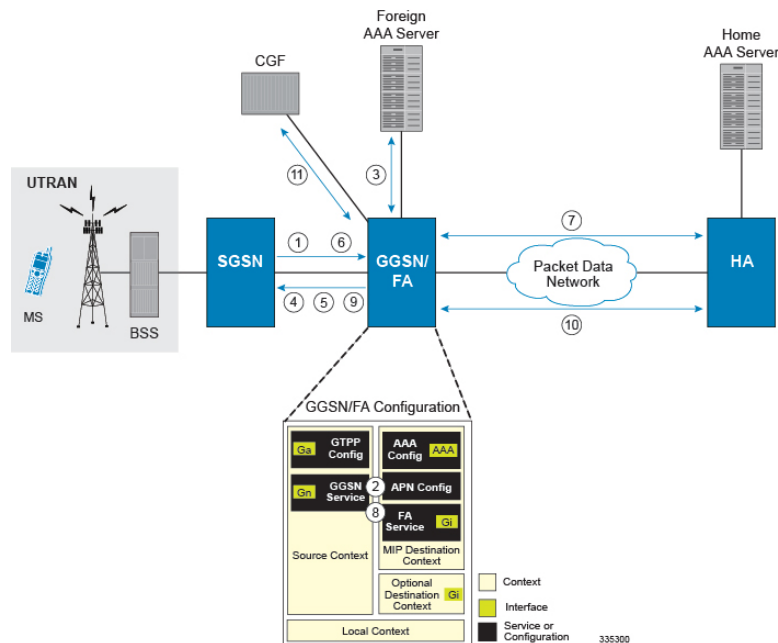
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. Important For this configuration, the destination context name should not match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 24: Call Processing When Using the system as a GGSN/FA



- 1 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.

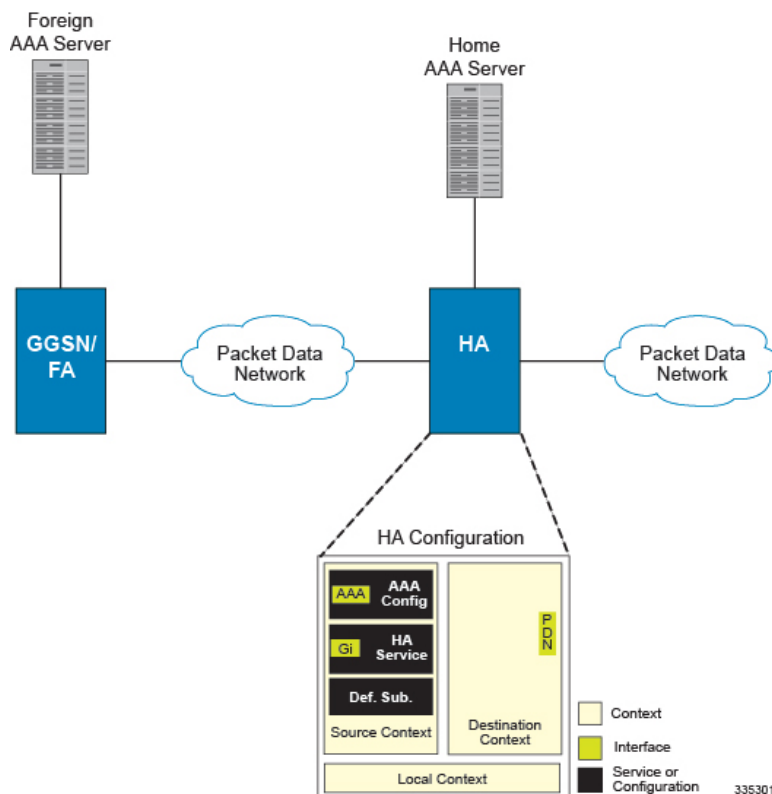
- 2 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
- 3 If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
- 4 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
- 5 The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more care-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
- 6 The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
- 7 The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. In response the HA sends a registration response to the FA containing the address assigned to the MS.
- 8 The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
- 9 The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
- 10 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
- 11 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Example 2: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a GGSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide GGSN/FA functionality.

The system's HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 25: Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Gi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 7: Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.

Required Information	Description
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number and can be any integer value from 1 to 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: <ul style="list-style-type: none"> • Always require authentication • Never require authentication Important The initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.

Required Information	Description
FA-to-HA Security Parameter Index Information	<p>FA IP address: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with.</p> <p>Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p>
	<p>Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p>Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>
	<p>Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.</p>
Mobile Node Security Parameter Index Information	<p>Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p>Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>
	<p>Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.</p>
	<p>Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.</p>

Required Information	Description
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	

Required Information	Description
Home RADIUS Authentication server	<p>IP Address: Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Home RADIUS servers are configured within the source context. Multiple servers can be configured and each can be assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>
Home RADIUS Accounting server (optional)	<p>IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	<p>Specifies the name of the egress context on the system that facilitates the Gi interfaces.</p> <p>Important For this configuration, the IP context name should be identical to the name of the destination context.</p>

Destination Context Configuration

The following table lists the information required to configure the destination context.

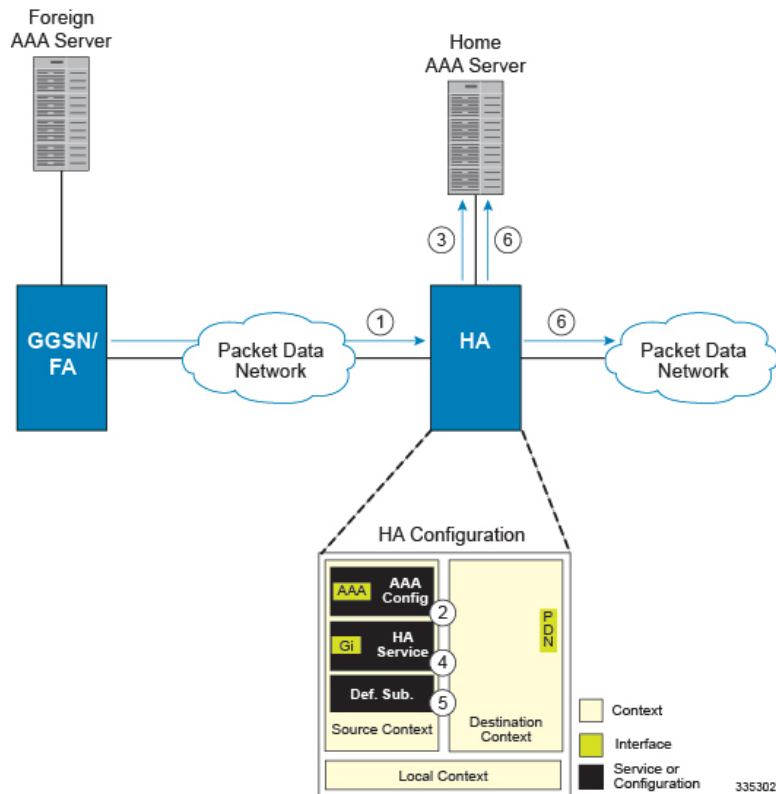
Table 8: Required Information for Destination Context Configuration 3

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. Important For this configuration, the destination context name should not match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 26: Call Processing When Using the system as an HA



- 1 A subscriber session from the FA is received by the HA service over the Gi interface.
- 2 The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the *Source* context.
- 3 The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
- 4 Upon successful authentication, the *Source* context determines which egress context to use for the subscriber session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
For this example, the system determines that the egress context is the *Destination* context based on the configuration of the *Default* subscriber.

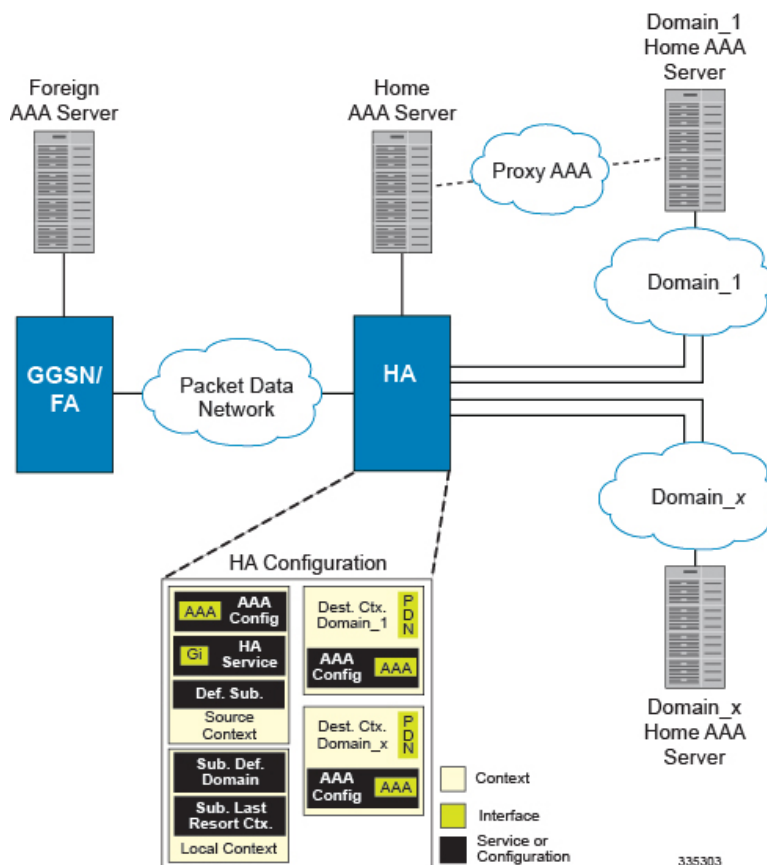
- 5 An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
- 6 Data traffic for the subscriber session is then routed through the PDN interface in the *Destination* context.
- 7 Accounting messages for the session are sent to the AAA server over the AAA interface.

Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could be owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

Figure 27: The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context will facilitate the HA service(s), and the Gi interface(s) to the FA(s). The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 9: Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gi Interface Configuration	
Gi interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.

Required Information	Description
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number and can be any integer value from 1 to 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: <ul style="list-style-type: none"> • Always require authentication • Never require authentication Important The initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.
FA-to-HA Security Parameter Index Information	FA IP address: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5 . A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	<p>Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p>Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>
	<p>Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.</p> <p>A hash-algorithm is required for each SPI configured.</p>
	<p>Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds.</p> <p>A replay-protection process is required for each mobile node-to-HA SPI configured.</p>
Maximum registration lifetime	<p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>
Maximum number of simultaneous bindings	<p>Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>
AAA Interface Configuration	
AAA interface name	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>AAA interfaces will be configured in the source context.</p>
IP address and subnet	<p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>

Required Information	Description
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	<p>IP Address: Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>

Required Information	Description
Home RADIUS Accounting server (optional)	<p>IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	<p>Specifies the name of the egress context on the system that facilitates the Gi interfaces.</p> <p>Important For this configuration, the IP context name should be identical to the name of the destination context.</p>

Destination Context Configuration

The following table lists the information required to configure the destination context. This information will be required for each domain.

Table 10: Required Information for Destination Context Configuration 11

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. NOTE: For this configuration, the destination context name should not match the domain name of a specific domain.
PDN Interface Configuration	

Required Information	Description
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	<p>IP Address: Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>

Required Information	Description
RADIUS Accounting server (optional)	<p>IP Address: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 11: Required Information for System-Level AAA Configuration

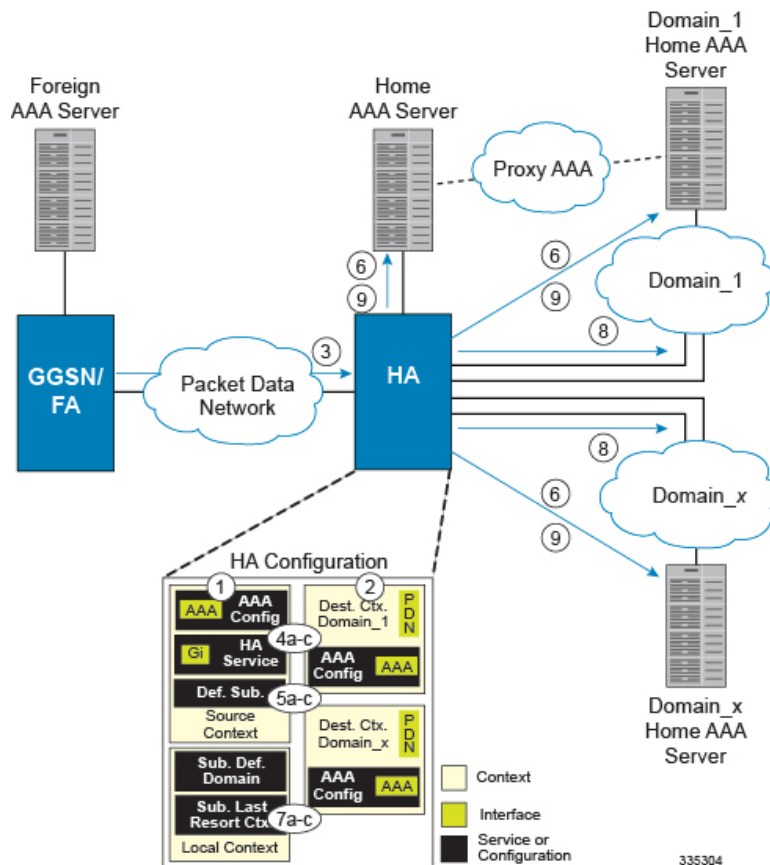
Required Information	Description
Subscriber default domain name	<p>Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access.</p> <p>Important The default domain name can be the same as the source context.</p>

Required Information	Description
Subscriber Last-resort context	<p>Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context .This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access.</p> <p>Important The last-resort context name can be the same as the source context.</p>
Subscriber username format	<p>Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are:</p> <ul style="list-style-type: none"> • @ • % • - • \ • # • / <p>Up to six username formats can be specified. The default is <i>username</i> .</p> <p>Important The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string, only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string <i>user!enterprise!spl</i>, the system resolves to the username <i>user!enterprise</i> with domain <i>isp1</i>.</p>

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 28: Call Processing When Using the system as an HA with a Single Source Context and Multiple Outsourced Destination Contexts



335304

- The system-level AAA settings were configured as follows:
 - Subscriber default domain name = *Domainx*
 - Subscriber username format = *username*
 - No subscriber last-resort context name was configured
- The subscriber IP context names were configured as follows:
 - Within the *Source* context, the IP context name was configured as *Domainx*
 - Within the *Domainx* context, the IP context name was configured as *Domainx*
- Sessions are received by the HA service from the FA over the Gi interface for *subscriber1Domain1*, *subscriber2*, and *subscriber3Domain37*.

- 4 The HA service attempts to determine the domain names for each session.
 - For *subscriber1*, the HA service determines that a domain name is present and is *Domain1*.
 - For *subscriber2*, the HA service determines that no domain name is present.
 - For *subscriber3*, the HA service determines that a domain name is present and is *Domain37*.
- 5 The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
 - For *subscriber1*, the HA service determines that a context was configured with a name (*Domain1*) that matches the domain name specified in the username string. Therefore, *Domain1* is used.
 - For *subscriber2*, the HA service determines that *Domainx* is configured as the default domain name. Therefore, *Domainx* is used.
 - For *subscriber3*, the HA service determines that no context is configured that matches the domain name (*Domain37*) specified in the username string. Because no **last-resort** context name was configured, the *Source* context is used.
- 6 The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
- 7 Upon successful authentication of all three subscribers, the HA service determines which destination context to use for each of the subscriber sessions. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
 - For *subscriber1*, the HA service receives the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute equal to *Domain1* as part of the Authentication Accept message from the AAA server on *Domain1*'s network. Therefore, *Domain1* is used as the destination context.
 - For *subscriber2*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Domainx* context. Therefore, the *Domainx* context is used as the destination context.
 - For *subscriber3*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Source* context. Therefore, the *Source* context is used as the destination context.
- 8 Data traffic for the subscriber session is then routed through the PDN interface in the each subscriber's destination context.
- 9 Accounting messages for the session are sent to the AAA server over the appropriate AAA interface.



CHAPTER

6

GGSN and Mobile IP Service in a Single System Configuration Example

This chapter provides information for several configuration examples that can be implemented on the system to support GGSN and Mobile IP data services in a single system.



Important

This chapter does not discuss the configuration of the local context. Information about the local context can be found in *System Administration Guide*.



Important

When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

- [Using the System as Both a GGSN/FA and an HA, page 173](#)

Using the System as Both a GGSN/FA and an HA

The system supports both GGSN and Mobile IP functionality. For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSNSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how a single system simultaneously supports both of these functions.

In order to support GGSN, FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context facilitates the following:

- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

- Access Point Name (APN) configuration

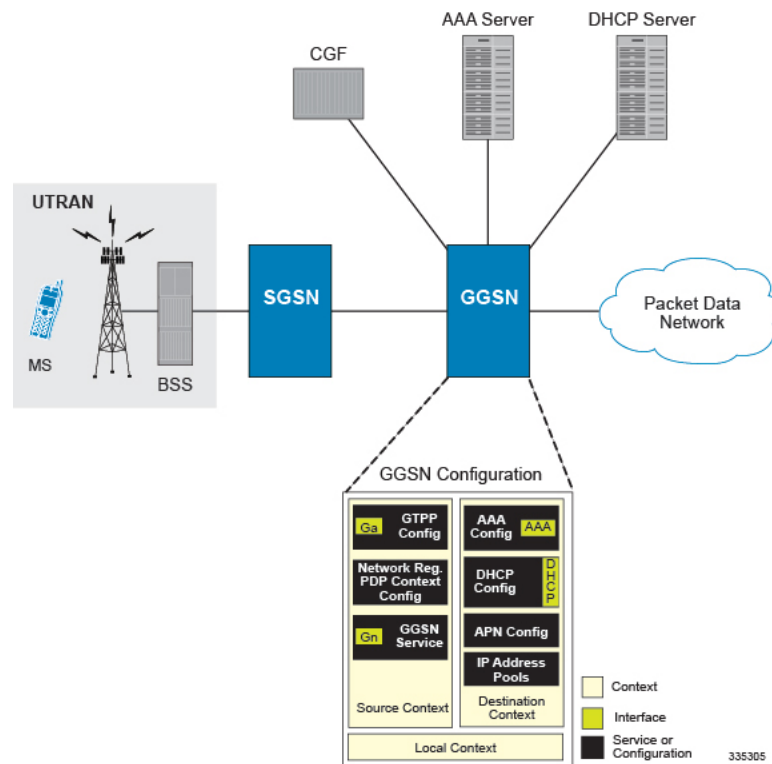
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

The Mobile IP destination context facilitates the following:

- FA Service(s)
- HA Service(s)
- Gi interface to the packet data network (PDN)
- ICC interface facilitating communication between the FA and HA services.

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts. In addition, Mobile IP and Proxy Mobile IP are supported for IP PDP contexts.

Figure 29: Simple and Mobile IP Support Within a Single System



Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the required information to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 12: Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.

Required Information	Description
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	Mobile Country Code (MCC): The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.

Required Information	Description
GGSN charging characteristics (CC) (optional)	<p>Behavior Bits: If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p> <p>Profile Index: If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). • Prepaid accounting can be disabled for a specified profile index. <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15</p>
PLMN policy	<p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)
Ga Interface Configuration	

Required Information	Description
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	IP address: The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	Priority: If more than one CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages: The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.

Required Information	Description
GCDR optional fields	<p>The following optional fields can be specified/configured in CDRs generated by the GGSN:</p> <ul style="list-style-type: none"> • diagnostics • duration-ms (the time specified in the mandatory Duration field is reported in milliseconds) • local-record-sequence-number • plmn-id
Network Requested PDP Context Support Configuration (optional)	
Activation Requirements	<p>IP address: The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.</p>
	<p>Destination context name: The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.</p>
	<p>International Mobile Subscriber Identity (IMSI): The IMSI of the mobile station.</p>
	<p>APN: The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.</p>
GSN-map node	<p>Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.</p>

Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 13: Required Information for Destination Context Configuration

Required Information	Description
Destination context name	<p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.</p> <p>Important For this configuration, the destination context name should not match the domain name of a specific APN.</p>
APN Configuration	

Required Information	Description
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. Important The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. Important The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.
IP address allocation method	Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods: <ul style="list-style-type: none"> • Dynamic: Address can be dynamically assigned from one of the sources: <ul style="list-style-type: none"> • Dynamic Host Control Protocol (DHCP) server: The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS. • Local address pools The system can be configured with local address pools. • Static: MS IP addresses can be permanently assigned. <p>By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.</p>
IP address pool name	If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.

Required Information	Description
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. When supporting Mobile IP, this is the name of the context containing the FA service configuration. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1000000. The default is 1000000.
PDP type	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: <ul style="list-style-type: none"> • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)
Mobile IP Configuration	<p>Home Agent IP Address: The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address.</p> <p>Parameters stored in individual profiles supersede parameters provided by the APN.</p> <p>Mobile IP Requirement: The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.</p>
DHCP Interface Configuration (optional)	
DHCP interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Gateway IP address	Used when configuring static routes from the DHCP interface(s) to a specific network.

Required Information	Description
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured .Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.
Lease Duration	Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. <ul style="list-style-type: none"> • Minimum Lease Time: Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds. • Maximum Lease Time: Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	<p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	<p>IP Address: Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>
RADIUS Accounting server (optional)	<p>IP Address: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.

Required Information	Description
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Gi Interface Configuration	
Gi interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	This is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.
Pool addresses, subnet mask and type	<p>The pool can consist of either of the following:</p> <ul style="list-style-type: none"> • An entire subnet configured using the initial address and the subnet mask • A range of addresses configured using the first and last IP addresses in the range <p>The pool can be configured as public, private, or static. Public pools can also be assigned a priority.</p>

Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 14: Required Information for Mobile IP Destination Context Configuration

Required Information	Description
Mobile IP Destination context name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system.</p> <p>Important For this configuration, the destination context name should not match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.</p>
ICC Interface Configuration	
ICC interface name	<p>The intra-context communication (ICC) interface is configured to allow FA and HA services configured within the same context to communicate with each other.</p> <p>The ICC interface name is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>ICC interface(s) are configured in the same destination context as the FA and HA services.</p>
IP address and subnet	<p>These will be assigned to the ICC interface(s).</p> <p>Multiple addresses (at least one per service) on the same subnet will be needed to assign to the same ICC interface.</p>
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical ICC interfaces.</p>
Gi Interface Configuration	

Required Information	Description
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.

Required Information	Description
Security Parameter Index (indices) Information	HA IP address: Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. Important The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.

Required Information	Description
HA service Configuration	
HA service name	<p>This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used.</p> <p>HA services are configured in the destination context.</p>
UDP port number for Mobile IP traffic	<p>Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.</p>
Mobile node re-registration requirements	<p>Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:</p> <ul style="list-style-type: none"> • Always require authentication • Never require authentication <p>Important The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"> • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.
FA-to-HA Security Parameter Index Information	<p>FA IP address: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with.</p> <p>Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p>
	<p>Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p>Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>
	<p>Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.</p>

Required Information	Description
Mobile Node Security Parameter Index Information	<p>Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>
	<p>Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>
	<p>Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.</p>
	<p>Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds.</p> <p>A replay-protection process is required for each mobile node-to-HA SPI configured.</p>
Maximum registration lifetime	<p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>
Maximum number of simultaneous bindings	<p>Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>
Default Subscriber Configuration	
"Default" subscriber's IP context name	<p>Specifies the name of the egress context on the system that facilitates the Gi interfaces.</p> <p>Important For this configuration, the IP context name should be identical to the name of the destination context.</p>

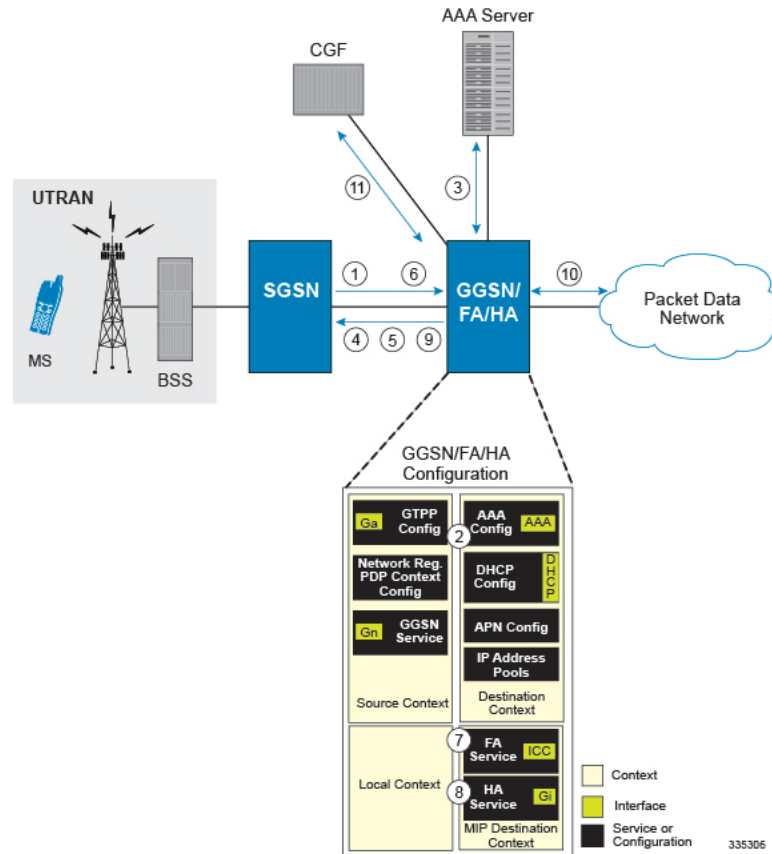
How This Configuration Works

This system configuration supports typical GGSN and Mobile IP functionality.

System operation for typical GGSN functionality behaves as described in *GGSN Configuration Example* chapter of this guide for each of the various call types. This section focusses on how this system configuration

functions to process a Mobile IP session. The following figure and the text that follows describe how this configuration works to process calls

Figure 30: Call Processing When Using the System as a GGSN, FA, and HA



- 1 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 2 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
- 3 If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
- 4 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
- 5 The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
- 6 The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address.

Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.

- 7 The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. The FA service communicates with the required HA service configured in the same context over the ICC interface. In response the HA sends a registration response to the FA containing the address assigned to the MS.
- 8 The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
- 9 The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
- 10 The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
- 11 Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.



Mobile-IP and Proxy-MIP Timer Considerations

This section is intended to provide a brief explanation of the considerations for lifetime, idle, and absolute timer settings that must be understood when setting up a system in a mobile IP or proxy mobile IP environment. In the Cisco ASR 5500 platform, there is not an explicitly defined MIP lifetime. The MIP lifetime is determined through various timers settings in the configuration and through radius attributes returned in an Access-Accept message.

This chapter contains the following topics:

- [Call Flow Summary, page 193](#)
- [Dealing with the 'Requested Lifetime Too Long' Error Code, page 195](#)
- [Controlling the Mobile IP Lifetime on a Per-Domain Basis, page 195](#)

Call Flow Summary

The following steps describe the call flow as regards the timers that affect a call initiated by the Mobile Node (MN).

- 1 PPP Negotiation:** A data call is initiated by beginning PPP. Once PPP is successfully established, the system will understand if the call is a mobile IP call or simple IP call. At this point, the system is not aware of the subscriber username and will use settings from the default subscriber template in the source context or the context defined by the "aaa default-domain subscriber" setting in the global configuration.
- 2 FA Agent Advertisement:** Once the system has determined the call is a Mobile IP call, the FA will send a Router Advertisement message with a Mobility Agent Advertisement extension. The Mobility Agent Advertisement includes a Registration Lifetime field. The value of this field will come from one of two places. The FA service has a configurable setting named "advertise reg-lifetime". The default value for this setting is 600. A setting in the default subscriber template called "timeout idle" is also a candidate. The default value for this setting is 0 (null). The smaller of these two configurable parameters is used as the Registration Lifetime value. Leaving the settings at the defaults will result in an advertised lifetime of 600.

Advertise Reg-Lifetime in FA Service	Timeout Idle in Subscriber Template	Resulting Advertised Registration Lifetime
600	0	600
600	900	600

Advertise Reg-Lifetime in FA Service	Timeout Idle in Subscriber Template	Resulting Advertised Registration Lifetime
3600	1200	1200

The device will receive the agent advertisement and send a MIP Registration Request. The device uses the advertised registration lifetime value as the requested MIP lifetime.

- 3 AAA Authentication and MIP Registration Request:** The next step in the MIP process will be to authenticate the user at the FA. It is at this stage where a failure condition can be introduced. If the Access-Accept message does not return any values related to timers, the subscribers MIP Registration Request is sent on to the HA.

If the Access-Accept message does include an attribute relating to Idle or Absolute timer the FA will evaluate the requested lifetime from the device to the value returned by the AAA. The FA will treat any Idle or Absolute timer value returned by the AAA as a maximum value and as such:

- If the requested MIP lifetime from the device is less-than than the returned radius attribute, the lifetime value is considered valid and the MIP Registration Request is forwarded on to the HA.
- If the requested MIP lifetime from the device is greater-than the returned radius attribute, the requested lifetime value is considered to be too long. The FA will send a MIP Registration Reply to the device with a response code of Error 69 - Requested Lifetime Too Long. In the reply message, the FA will populate the Lifetime value with the maximum acceptable lifetime. The device may send a new MIP request with this new lifetime value.

MIP Lifetime Requested by Device	Idle-Timer Value in Access-Accept	Resulting MIP Lifetime Request in MIP Request to HA
3600	(Not Returned)	3600
3600	7200	3600
3600	1800	Failure - Error 69

- 4 HA Process MIP Request:** The HA has now received a Mobile IP Registration request forwarded by the FA on behalf of the device. The MIP request contains the username and the requested lifetime (as well as other parameters). The HA will take this lifetime request and compare it to the configurable parameters associated with the HA service and associated configurations. The HA will use the username to determine which subscriber template to use for subscriber specific settings.

The parameters the HA uses to determine the MIP lifetime are the requested lifetime, the "reg-lifetime" setting in the HA service and the "timeout idle" setting in the subscriber template. If the requested MIP lifetime is lower it is be sent back to the mobile; if the MIP lifetime is higher the system sends back an RRQ accept with the lifetime set to 5 seconds less than the lower of the idle or absolute timeout for the user.

MIP Lifetime Requested by Device	Timeout Idle/Absolute in Subscriber Template	Reg-Lifetime Value in HA Service	MIP Lifetime Returned to Mobile Device
3600	0(default)	7200	3600
3600	7200	1805	1800

MIP Lifetime Requested by Device	Timeout Idle/Absolute in Subscriber Template	Reg-Lifetime Value in HA Service	MIP Lifetime Returned to Mobile Device
3600	1705	3600	1700

PDSN/FA			HA		
Advertise Reg-Lifetime in FA Service	Timeout Idle/Absolute in Subsc. Template (Source Context)	Idle-Timer Value in Access-Accept	Timeout Idle/Absolute in Subscriber Template(HA Context)	Reg-Lifetime Value in HA Service	Resulting Lifetime Value sent to Mobile Device
600	0(default)	(not returned)	0(default)	7200	600
1800	900	7200	7200	1805	900
3600	1200	3600	1705	3600	1200
1500	3600	1500	0(default)	3600	1500
3600	0(default)	(not returned)	0(default)	2405	2400
3600	0(default)	(not returned)	2005	3600	2000
65534	0(default)	7200	0(default)	3600	Lifetime Too Long

Dealing with the 'Requested Lifetime Too Long' Error Code

In some configurations, a roaming partner may return an "Idler-Timer" attribute in an access-accept whose value is smaller than what a carrier may have configured for its own subscribers. This will result in a "Requested Lifetime Too Long" error message being returned to the device. There are several ways to correct this. One is to use a setting in the FA service configuration. Using the "no limit-reg-lifetime" in the FA service configuration will tell the FA service to allow the MIP lifetime to be greater than the Idle or Absolute timers. The FA will not send Error 69 and continue to process the call. The lifetime value in the MIP Request sent to the HA will still be what was determined in Phase 2.

Controlling the Mobile IP Lifetime on a Per-Domain Basis

The system does not support the configuration of the MIP lifetime timer on per- domain (context) basis. However, a domain-wide lifetime timer can be achieved by configuring the idle-timeout attribute for the default subscriber for each domain.



Important

Mobile IP lifetime settings can be controlled on a per-domain basis **only** in deployments for which the idle timeout attribute for individual subscriber profiles is **not** used during operation.

In this configuration, the value of the registration lifetime sent by the system in Agent Advertisements is selected by comparing the configured FA Agent Advertisement lifetime setting, and the idle and/or absolute timeout settings configured for the domain's default subscriber. If the value of the idle and/or absolute timeout parameter is less than the Agent Advertisement lifetime, then the system provides a registration lifetime equal to 5 seconds less than the lowest timer value.

If the idle timeout attribute is configured in individual subscriber profiles, per-domain lifetime control is not possible. In this case, the registration lifetime configured for the FA must be the lower of the two values.



Important

Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

The following is an example CLI command sequence used to configure the Mobile IP lifetime on a per-domain basis.

```
configure
  context <aaa_context_name>
    subscriber default
      ip context-name <abc>
      exit
    subscriber name <ptt.bigco.com>
      timeout idle <3605>
      ip context-name <abc>
      exit
    subscriber name <bigco.com>
      timeout idle <7205>
      ip context-name <abc>
      exit
    domain <ptt.bigco.com> default subscriber <ptt.bigco.com>
    domain <bigco.com> default subscriber <bigco.com>
  end
configure
  context <ha_context_name>
    subscriber default
      exit
    ha-service <ha>
      idle-timeout-mode normal
      reg-lifetime <7200>
    end
configure
  context <fa_context_name>
    fa-service <fa>
      advertise reg-lifetime <7200>
    end
```

In the example above, two domains (ptt.bigco.com and bigco.com) are configured. The default subscribers are defined for the two domains respectively. The desired operation requires a Mobile IP lifetime of 1 hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of 2 hours (7200 secs) for the bigco.com domain.

Whenever a subscriber session belonging to the ptt.bigco.com domain arrives, the system uses a Mobile IP lifetime timer value equal to 5 seconds less than the idle timeout configured for the default subscriber because the configured value is less than the registration lifetime value configured for the Agent Advertisement. 5 seconds less than the configured value of 3605 seconds equals 3600 seconds which meets the desired operation.

Whenever a subscriber session belonging to the bigco.com domain arrives, the system uses the configured registration lifetime value as the Mobile IP lifetime in Agent Advertisements because it is less than the configured idle timeout in the default subscriber's profile.

As a general rule, the registration lifetime value on the agent **must** be configured as the highest Mobile IP lifetime that is desired for a subscriber. (In the above example, it would be the subscriber bigco.com.)

Another important factor to consider is that the idle timeout value should be reset on receipt of a renewal request. To support this operation, the system provides the **idle-timeout-mode** configurable in the HA service. The following modes are supported:

- **normal**: Resets the idle timeout value on receipt of Mobile IP user data and control signaling
- **aggressive**: Resets the idle timeout value on receipt of Mobile IP user data only (this is the default behavior)
- **handoff**: Resets the idle timeout value on receipt of Mobile IP user data and upon inter-AGW handoff or inter access technologies

The following optional modifier is also supported:

- **upstream-only**: Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.



Session Tracing

This chapter provides information on subscriber session trace functionality that allows an operator to trace subscriber activity at various points in the network and at various level of detail. Subscriber session tracing is supported on the following UMTS/EPC GW network elements:

- GGSN
- P-GW
- SAEGW
- S-GW



Important

For detailed information for session tracing on the MME, refer to the *MME Administration Guide*.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

This chapter includes a feature description, configuration procedures, monitoring commands, and a session tracing file example.

- [Session Tracing Overview](#), page 199
- [Configuring Session Trace Functionality](#), page 203
- [Monitoring the Session Trace Functionality](#), page 215
- [Supported SAEGW Session Trace Configurations](#), page 215
- [Session Trace File Example](#), page 219

Session Tracing Overview

Session Trace capability enables an operator to trace subscriber activity at various points in the network and at various levels of detail. The trace can be subscriber initiated (that is, signaling based) or management

initiated from the CLI (Command Line Interface) and can be propagated throughout the access cloud via the various signaling interfaces available to the UMTS/EPC network element.

Essentially, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a User Equipment (UE) connects to the access network.

All monitored activity is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a File Transfer Protocol (FTP) or secure FTP (SFTP) connection.

**Important**

Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

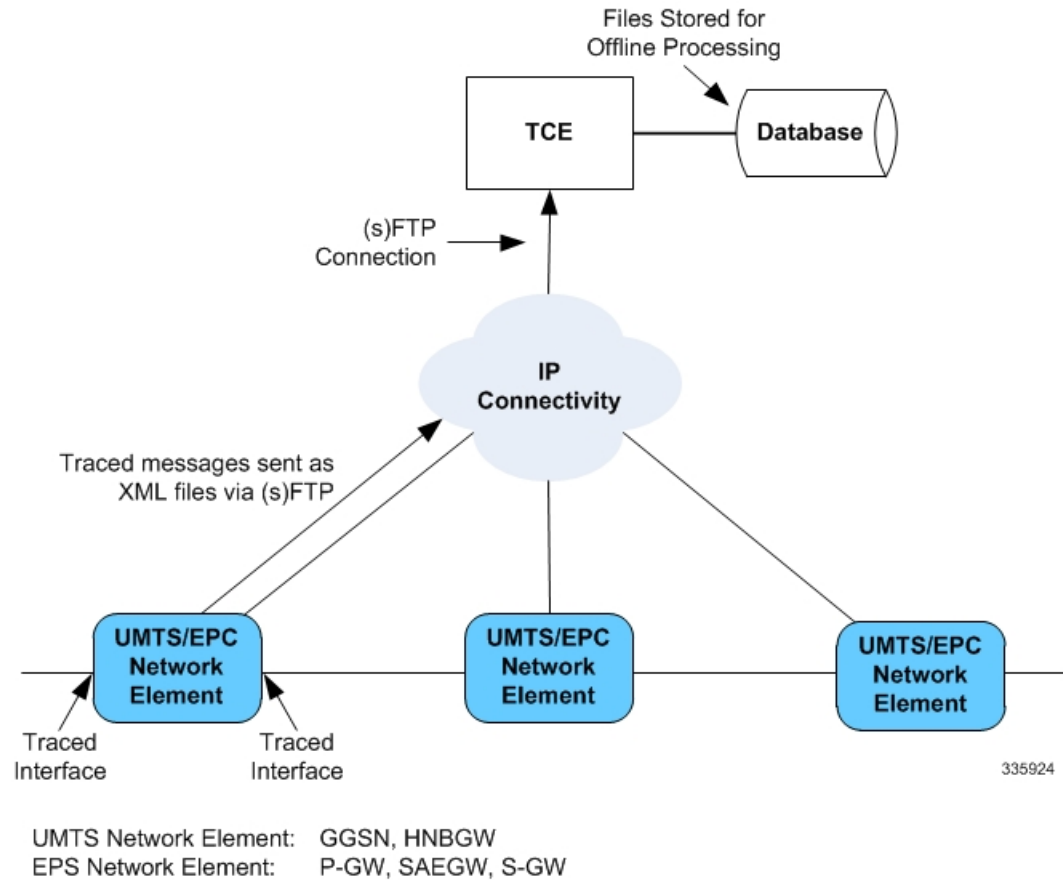
**Important**

For 19.2 and prior StarOS releases, both the FTP and SFTP options are available. In release 20.0 and higher trusted StarOS builds only the SFTP option is supported; FTP is not supported for the Session Trace function in release 20.0 and higher trusted StarOS builds.

As can be seen in the following illustration, of the three Network Elements (NEs) shown, one NE is actively tracing data on one or more interfaces. All data collected is stored as files in an XML format and then transferred

to the collection entity using (S)FTP or FTP. Note that IPv4 or IPv6 connectivity is required between the NE and the TCE in order to transfer the files.

Figure 31: Session Tracing Architecture



Session Trace Types

There are three types of session trace functions available.

- **Management Trace:** The operator sends an activation request via the CLI directly to the UMTS/EPC network element where the trace is to be initiated. The network element establishes the trace session and waits for a configured trigger event to start actively tracing. When management-initiated trace activations are executed at the network element, they are never propagated to other NEs whether or not it is involved in the actual recording of the call.
- **Random Trace:** Enables or disables the subscriber session trace functionality based on a the random trace on the UMTS/EPC network element. The trace control and configuration parameters are configured directly in the specified network element through the **random trace** CLI command. There is no propagation of trace parameters in random based trace activation. This NE shall not propagate the received data to any other NEs whether or not it is involved in the actual recording of the call. If enabled, the subscriber selection will be based on random logic all instances of session on the specified UMTS/EPC network element.

- **Signaling Trace:** With a signaling based activation, the trace session is indicated to the UMTS/EPC network element across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active). Signaling based activations are always propagated to neighboring NEs even if the current NE does not participate in the trace (either they not enabled by configuration or not present in the configured trace parameters).

**Important**

Note that the maximum number of unique International Mobile Subscriber Identification (IMSI) numbers or International Mobile Equipment Identification (IMEI) numbers cannot exceed 32; however, each NE can trace all 32 unique IMSI/IMEIs.

**Caution**

Session tracing is a resource intensive application in terms of CPU utilization and will affect call rates and data throughput when in use. The use of this feature in a production network should be restricted to minimize the impact on existing services.

Session Trace Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, an (S)FTP connection to the Trace Collection Entity (TCE) is established if one does not already exist. The NE will store up to 2 MB of XML data on its local disk to allow for the (S)FTP connection to be established and the files to be pushed to or pulled from the TCE.

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity waits until the start trigger occurs (typically when the subscriber/UE under trace initiates a connection). A failure to activate a trace (due to the maximum being exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure.

Session Trace Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Data Collection

Data collection is done inline by each of the NEs. In order to reduce the overhead on a per-control packet basis, a copy of the entire packet is made and stored into an internal database (DB) of packets.

The local internal path for the trace database is `/hd-raid/trace`.

This storage is done regardless of the trace depth. After xx bytes (or xx messages) have been stored or a configurable number of seconds have elapsed, all cached data is encoded in the standard XML format and written out to a file to be forwarded to/pulled from the TCE. If there is no TCE active, the UMTS/EPC network

element will continue to cache data and create trace files as long as there is space available before stopping the trace recording session. Once the connection to the TCE becomes active, all cached data will be sent immediately to the TCE.

Data Forwarding

When a session is activated, the IP address of the TCE is supplied in the session activation request. Upon activation and if the push mode is used, a check is made to see if there is already an (S)FTP connection to the TCE. If so, it is used for all traffic associated with this trace session. If not, an (S)FTP connection is made to the TCE using the supplied IP address. Data is buffered locally and trace files generated until the connection is established. Once the connection is established, all previously created trace files are sent to the TCE. Note that the (S)FTP connection is established to the TCE at session activation regardless of whether or not a trace recording session has been triggered. The (S)FTP connection is maintained until the trace session is deactivated.

Note the following:

- If a default TCE IP Address is supplied when the trace capability is configured, a default (S)FTP connection is made to the remote TCE.
- The TCE can be reachable either via IPv4 or IPv6 addressing. The supplied TCE address indicates the version.
- If the push mode is not used, the files are stored on the local hard drive (**/hd-raid/trace**) and must be pulled off by the TCE using FTP or SFTP.

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added for the Session Trace feature:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

Configuring Session Trace Functionality

Configuring Session Trace on the UMTS/EPC network element consists of the following:

- 1 [Enabling Session Tracing, on page 204](#)
- 2 [Configuring a Session Trace Template for the Management Trace Function, on page 205](#)
- 3 [Configuring a Management Session Trace, on page 209](#)
- 4 [Configuring a Signaling Session Trace, on page 210](#)

5 [Configuring a Random Trace, on page 211](#)

The trace files can be stored locally, or pushed to a Trace Collection Entity (TCE) specified in the various trace commands.



Important

Not all combinations of Session Trace configuration types are allowed on the SAEGW. For details on the supported session trace configuration types, refer to [Supported SAEGW Session Trace Configurations, on page 215](#) in this document.

Enabling Session Tracing

Session Tracing functionality must first be enabled before a specific management, random, or signaling session trace can be configured.

The following commands enable or disable the subscriber session trace functionality based on a specified subscriber device or ID on one or all instances of a session on a specified UMTS/EPC network element.

Use the following example to enable session tracing on the UMTS/EPC network element:

config

```
session trace network-element { all | ggsn | hnbgw | mme | pgw | saegw | sgw } [ file-type <a-type |
b-type> ] tce-mode none | push transport ftp | sftp username username encrypted password password
path directory_path collection timer ctimer_value
end
```

Notes:

- **session trace network-element** : Enables Session Tracing functionality on the specified network element. To enable session tracing for all supported network elements, enter **all**.
- **file-type { a-type | b-type }** : Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. Note that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs. The default is **a-type**.
- **tce-mode** : Specifies that trace files are stored locally and must be pulled by the TCE (**none**) or trace files are pushed to the TCE (**push**). The default is **none**.
- **transport** : Specifies the method by which the trace files are pushed to the TCE (either **ftp** or **sftp**.) The default is **sftp**.
- **username**: Must be specified if the **tce-mode** is **push**.
- **password**: Must be specified if the **tce-mode** is **push**.
- **encrypted**: Specifies that the password used to push files to the TCE server will be encrypted.
- **password**: Specifies the password to use to push files to the TCE server. The user name can be from 1 to 31 alphanumeric characters.
- **collection-timer**: Specifies the amount of time, in seconds, to wait from initial activation/data collection before data is reported to TCE. The default is 10 seconds.

- **retry-timer:** Specifies the amount of time, in seconds, to wait before retrying a file transfer if the previous transfer failed. The default is 60 seconds.

Example:

```
session trace network-element saegw tce-mode push transport sftp path /SessionTrace username
root encrypted password 5c4a38dc2ff61f72 collection-timer 5
```

Verifying that Session Tracing is Enabled

Use the following example to verify that session tracing functionality is enabled on the UMTS/EPC network element:

show session trace statistics

The output indicates for which NEs session tracing is enabled, and also indicates the configured trace type, where applicable. For example:

```
Network element status:
  MME:      Enabled      Cell-Trace: Disabled
  S-GW:     Enabled
SAEGW Enabled
  PGW:      Trace-Type: None
  SGW:      Trace-Type: None
```

Disabling Session Trace Functionality

Use the following example to disable session tracing functionality:

config

```
no session trace network-element { all | ggsn | hnbgw | mme | pgw | saegw | sgw }
end
```

Configuring a Session Trace Template for the Management Trace Function

Operators must create a template for a management trace in Global Configuration Mode. Management traces executed in Exec mode will use the template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

Note that to activate subscriber session traces for specific IMSI/IMEI, the operator will use the Exec mode **session trace subscriber** command specifying a pre-configured template and the IMSI/IMEI, trace reference, and TCE address.

Use the following example to configure a template for use with the **session trace subscriber** command:

config

```
template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name
template_name
```

Once this command is entered, the user is placed in *Session Trace Template Configuration Mode*. In this mode, the operator selects the interfaces to be traced for the selected network element.



Important

The options available in *Session Trace Template Configuration Mode* are dependent on the network element selected in the previous command.

For the **GGSN**, **MME**, **P-GW** and **S-GW**, enter the following command in *Session Trace Template Configuration Mode*:

```
interface interface_name
end
```

For the **SAEGW**, enter the following command in *Session Trace Template Configuration Mode*:

```
{ func-pgw | func-sgw } interface interface_name
end
```

- Notes: The available UMTS/EPC network elements provide various interface options for the session trace template.

GGSN

Available **ggsn** interfaces include:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

HNBGW

Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the iucs interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the iups interface between the HNB-GW and the SGSN.

MME

Available **mme** interfaces include:

- **all**: Specifies that all MME interfaces are to be traced.
- **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s13**: Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.

- **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

P-GW

Available **pgw** interfaces are:

- **all**: Specifies that all available P-GW interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

SAEGW

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

- Available **func-pgw interface** options are:
 - **all**: Specifies that all available **func-pgw** interfaces are to be traced.
 - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
 - **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.
 - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.

- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
 - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
 - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
 - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
 - **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
 - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- Available **func-sgw interface** options are:
 - **all**: Specifies that all available **func-sgw** interfaces are to be traced.
 - **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
 - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
 - **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
 - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
 - **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

S-GW

The available **sgw** interfaces are:

- **all**: Specifies that all available S-GW interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

Verifying the Session Trace Template Configuration

To verify the session trace configuration, enter the following command in Exec Mode.

```
show session trace template network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } all
```

The output provides the template name, the NE type, and all interfaces configured for tracing.

Disabling the Session Trace Template Configuration

Use the following example to disable the session trace template configuration:

```
no template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw }
```

Disabling the Session Trace Template Configuration per Network Element and Subscriber

To disable the session trace template per network element and subscriber:

```
no session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name  
template_name { imsi id | imei id } trace-ref trace_ref_value collection-entity ip_address
```

Configuring a Management Session Trace

Session tracing functionality must be enabled before a management trace can be configured. Refer to [Enabling Session Tracing, on page 204](#) for the procedure.

To configure a management session trace on the UMTS/EPC network element from Exec Mode:

```
session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name  
template_name { imei id | imsi id } { all | interface } } trace-ref id collection-entity ip_address
```

Notes:

- **template-name:** Specifies the name of the session trace template to use for this session trace. Session trace templates are configured in *Global Configuration Mode* using the **template-session-trace** command. Management traces executed in Exec mode will use the specified template.
- **imsi id:** Specifies the International Mobile Subscriber Identification Number for the subscriber.
- **imei id:** Specifies the International Mobile Equipment Identification number for the subscriber.
- **trace-ref:** Specifies the Trace Reference for this subscriber management trace. It must be composed of the Mobile Country Code (MCC) + the Mobile Network Code (MNC) + a 3 byte octet string Trace ID. Example: 31001212349.
- **collection-entity:** Specifies the IP address of the Trace Collection Entity (TCE) to which the trace file generated will be sent. The IP address must be in IPv4 format.

Example:

The following is a complete example showing the configuration of a subscriber management trace for all S-GW and P-GW interfaces. It consists of enabling session tracing on the SAEGW, creating the session trace template for all S-GW and P-GW interfaces, and then executing the subscriber management trace for a specific IMSI using the template.

```
config  
session trace network-element saegw
```

```

end
config
  template-session-trace network-element saegw template-name saegw_all
    func-pgw interface all
    func-sgw interface all
  end
session trace subscriber network-element saegw template-name saegw_all imsi 123456789012345
trace-ref 123456789012 collection-entity 1.1.1.1

```

Verifying the Management Trace Configuration

To verify that the management trace configuration for the subscriber is enabled, enter the **show session trace statistics** command from Exec Mode. Verify that the correct NE(s) show their Network element status as **Enabled**. For example:

```

SAEGW Enabled
      PGW:                      Trace-Type: M
      SGW:                      Trace-Type: M

```

Use the following example to verify that specific parameters have been activated for the subscriber management trace:

```

show session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace-ref
trace_ref_value

```

The output fields show the NE Type and the Trace Type configured for each network element. Below is sample output for an SAEGW management trace configuration:

```

NE Type: SAEGW
      PGW:                      Trace-Type: M
      SGW:                      Trace-Type: M
.....
Traced Interfaces:
PGW:
    <P-GW interfaces configured for the trace.>
SGW:
    <S-GW interfaces configured for the trace.>

```

Disabling the Management Trace Configuration

To disable the management trace configuration from Exec Mode:

```

no session trace subscriber network element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace ref
trace_ref_value

```

Configuring a Signaling Session Trace

Session trace functionality must be enabled before a signaling session trace can be configured. Refer to [Enabling Session Tracing, on page 204](#) for the procedure.

To configure a signaling session trace:

```

session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw | func-pgw | func-sgw | |
sgw }

```

Notes:

- **func-pgw**: Enables tracing of the P-GW signaling under the SAEGW
- **func-sgw**: Enables tracing of the S-GW signaling under the SAEGW

- If neither **func-sgw** or **func-pgw** is specified, then the signaling trace will be performed for all P-GW and S-GW interfaces of the SAEGW.
- **collection-entity**: Specifies the IPv4 or IPv6 address of the Trace Collection Entity (TCE) to which the trace files are sent.

Example:

This example configures a signaling session trace for all S-GW and P-GW interfaces under an SAEGW:

```
session trace signaling network-element saegw
```

Verifying the Signaling Session Trace Configuration

To verify the signaling session trace configuration:

show session trace statistics

Look for the following fields to verify the signaling trace configuration. For example:

```
Network element status:
.....
SAEGW Enabled
      PGW:                      Trace-Type: S
      SGW:                      Trace-Type: S
```

Disabling the Signaling Session Trace

To deactivate signaling trace on the SAEGW:

```
no session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw [ func-pgw | func-sgw ]
| sgw }
```

Configuring a Random Trace

Session trace functionality first must be enabled on the UMTS/EPC network element before a random trace can be configured. Refer to [Enabling Session Tracing, on page 204](#) in this chapter for the procedure.

The following command enables or disables the subscriber session trace functionality based on a random trace on the UMTS/EPC network element. If enabled, the subscriber selection will be based on random logic for all instances of session on a specified network element.

To configure a random session trace:

```
session trace random range network-element { ggsn | hnbgw | pgw | saegw | sgw [ func-pgw | func-sgw ] }
interface [ all | interface ] collection-entity ipv4_address
```

Notes:

- **session trace random range**: Enables a random trace for a specified number of subscribers. Valid entries are from 1 to 1000 subscribers.
- **{ ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] }**: Specifies that the random trace is enabled for the selected network element.
- **func-pgw**: Enables random tracing of the P-GW interfaces under the SAEGW.
- **func-sgw**: Enables random tracing of the S-GW interfaces under the SAEGW.
- If neither **func-pgw** or **func-sgw** are specified, random tracing will occur for both the P-GW and S-GW.

- **interface**: Specifies the network interfaces for the random trace. Interfaces available depend on the network element type selected.

GGSN

Available **ggsn** interfaces are:

- **all**: Specifies that all available GGSN interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

HNBGW

Available **hnbgw** interfaces are:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the **iucs** interface between the HNB-GW and the Mobile Switching Center (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the **iups** interface between the HNB-GW and the SGSN.

P-GW

Available P-GW interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).

- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

SAEGW

The interfaces that can be traced on the SAEGW are broken down by the interfaces available on a P-GW configured under an SAEGW (**func-pgw**), and the interfaces available on a S-GW configured under an SAEGW (**func-sgw**).

Available SAEGW **func-pgw** interface options are:

- **all**: Specifies that all **func-pgw** interfaces configured under an SAEGW are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- **gy**: Specifies that the interface where the trace will be performed is the GTPP based online charging interface between P-GW and online charging system.

Available SAEGW **func-sgw** interfaces are:

- **all**: Specifies that all available **func-sgw** interfaces under an SAEGW are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.

- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

S-GW: Available **sgw** interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.
- **collection-entity** specifies the IPv4 address of the Trace Collection Entity (TCE)

Example:

To enable random tracing on a range of 40 SAEGW subscribers on all S-GW interfaces and the s5 interface of the P-GW in the SAEGW, enter the following sample command:

```
session trace random 40 network-element saegw func-pgw interface s5 func-sgw interface all collection-entity 1.1.1.1
```

Verifying the Random Trace Configuration

To verify the random session trace configuration:

show session trace statistics

Look for the fields that verify that Random Session Trace has been enabled for the network element. For example:

```
Network element status:
...
SAEGW Enabled
    PGW:                      Trace-Type: R
    SGW:                      Trace-Type: R Configured-Random: 40
```

Disabling the Random Trace for a Specific Network Element

To disable random session tracing for a specific network element:

```
no session trace random network-element { ggsn | hnbgw | pgw | saegw | sgw [ func-pgw | func-sgw ] }
```

Monitoring the Session Trace Functionality

This section provides information on commands you can use to monitor the session trace functionality

show session trace statistics

This command provides high-level statistics on the current use of the session trace functionality, including:

- Number of current trace sessions
- Number of total trace sessions
- Total sessions activated
- Number of activation failures
- Number of sessions triggered
- Total messages traced
- Number of current TCE connections
- Total number of TCE connections
- Total number of files uploaded to all TCEs

show session trace subscriber network-element trace-ref

This command shows detailed information about a specific trace, based on the trace-ref value of the session and network element type. It includes activation time, IMSI, start time, number of trace messages, and total number of files created. It also lists the interfaces that this session trace is configured to trace.

show session trace trace-summary

This command provides the trace-ref value of all session traces, broken down by network element type.

show session trace tce-summary

This command provides the IP address and index information for all configured TCEs.

show session trace tce-address

This command provides detailed information about a specific TCE, including IP address, start time, and total number of files uploaded.

Supported SAEGW Session Trace Configurations

Different tracing configurations are supported on the SAEGW. The different combinations of session tracing types depend on Call Type, Trace Type, and whether the operator would like to configure a Func-SGW and/or a Func-PGW trace.

Note the following:

- M = Management

- R = Random
- S = Signaling

Table 15: Supported Session Trace Configurations on the SAEGW

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
M	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	When M traces are enabled for Func-SGW, Func-PGW and call type Collapsed both S-GW control messages (gtpv2) and P-GW control messages shall be traced in 1 SAEGW trace file.
R	R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	S	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M+S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	When M+S traces are enabled for Func-S-GW, Func-P-GW and call type collapsed both -SGW control messages (gtpv2) and P-GW control messages shall be traced in 2 SAEGW trace files. One Trace file due to Management and other due to Signaling. Both files have the same contents.
M+R	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
S	R	Collapsed	No	No	None	Not a valid trace configuration

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
R	S	Collapsed	No	No	None	Not a valid trace configuration
M	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M	Collapsed	No	Yes	1 SAEGW trace file generated	
M	S	Collapsed	No	Yes	1 SAEGW trace file generated	
S	M	Collapsed	Yes	No	1 SAEGW trace file generated	
M+S	M	Collapsed	Yes	No	2 SAEGW trace files generated	P-GW Trace is not generated
M	M+S	Collapsed	No	Yes	2 SAEGW trace files generated, but S-GW trace not generated	S-GW Trace is not generated
M+S	S	Collapsed	Yes	Yes	2 SAEGW trace files generated	
S	M+S	Collapsed	Yes	Yes	2 SAEGW trace files generated	
M+R	M	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M	M+R	Collapsed	Yes	Yes	1 SAEGW trace file generated	
M+R	R	Collapsed	Yes	No	1 SAEGW trace file generated	
R	M+R	Collapsed	No	Yes	1 SAEGW trace file generated	
M	n/a	Pure S	Yes	No	1 SAEGW trace file generated	Config for func-P-GW is not applicable for Pure S calls

Func-S-GW Trace Config	Func-P-GW Trace Config	Call Type	S-GW Trace?	P-GW Trace?	Output	Comments
S	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
M+S	n/a	Pure S	Yes	No	2 SAEGW trace files generated	
M+R	n/a	Pure S	Yes	No	1 SAEGW trace file generated	
R+S	n/a	Pure S	No	No	None	Not a valid trace configuration.
n/a	M	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	S	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	M+S	Pure P	No	Yes	2 SAEGW trace file generated	
n/a	M+R	Pure P	No	Yes	1 SAEGW trace file generated	
n/a	R+S	Pure P	No	Yes	None	Not a valid trace configuration

Session Trace File Example

This section provides an example of a signaling trace file.

Figure 32: Signaling Trace File Example (1 of 3)

```
<<<<OUTBOUND 10:04:53:997 EventId:141005(3)
[MME-S11]GTPv2C Tx PDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x000004D3, Message type: EGTP_TRACE_SESSION_ACTIVATION (0x47)
Sequence Number: 0x000401 (1025)
GTP HEADER
    Version number: 2
    TEID flag: Present
    Piggybacking flag: Not present
    Message Length: 0x003A (58)

INFORMATION ELEMENTS
    IMSI:
        Type: 1 Length: 8 Inst: 0
        Value: 123456789012345
        Hex: 0100 0800 2143 6587 0921 43F5

    Trace Info:
        Type: 96 Length: 34 Inst: 0
        Value:
            MCC: 123
            MNC: 456
            Trace Id: 03039

    Triggering Event: 1/0: Event shall be traced / not traced.
    MSC Server:
        SS: 0
        HANDOVERS: 0
        LU/IMSI ATT/DET: 0
        MO & MT SMS: 0
        MO & MT CALLS: 0

    MGW:
        CONTEXT: 0

    SGSN:
        MBMS CONTEXT: 0
        RAU/GPRS ATT/DET: 0
        MO & MT SMS: 0
        PDP CONTEXT: 0

    GGSN:
        MBMS CONTEXT: 0
        PDP CONTEXT: 0

    MME:
        HANDOVERS: 1
        BEARER ACT/MOD/DEL: 1
        UE INIT PDN DISC: 1
        INIT ATT/TAU/DET: 1
        SERVICE REQUEST: 1
        UE INIT PDN CON REQ: 1
```

335925

Figure 33: Signaling Trace File Example (2 of 3)

```

PGW:
    BEARER ACT/MOD/DEL: 1
    PDN CONN TERMINATE: 1
    PDN CONN CREATE: 1

SGW:
    BEARER ACT/MOD/DEL: 0
    PDN CONN TERMINATE: 0
    PDN CONN CREATE: 0

List of NE Types: 1/0: Trace Session activated/ not activated.
SGW: 0
MME: 1
EMSC: 0
RNC: 0
GGSN: 0
SGSN: 0
MGW: 0
MSC-S: 0
ENODEB: 1
PDN-GW: 1

Trace Depth:
Value: 5 (MAXIMUM w/o Vendor Specific Extension)

List of Interfaces: 1/0: Interface will be traced/ not traced.
MSC Server:
    CAP: 0
    MAP-F: 0
    MAP-E: 0
    MAP-B: 0
    MAP-G: 0
    MC: 0
    IU: 0
    A: 0
    MAP-C: 0
    MAP-D: 0

MGW:
    IU-UP: 0
    Nb-UP: 0
    MC: 0

SGSN:
    GE: 0
    GS: 0
    MAP-GF: 0
    MAP-GD: 0
    MAP-GR: 0
    GN: 0
    IU: 0
    GB: 0

GGSN:
    GMB: 0
    GI: 0
    GN: 0

```

335926

Figure 34: Signaling Trace File Example (3 of 3)

RNC:

UU: 0
IUB: 0
IUR: 0
IU: 0

BMSC:

GMB: 0

MME:

S11: 1
S10: 1
S6A: 1
S3: 1
S1-MME: 1

SGW:

GXC: 0
S11: 0
S8B: 0
S5: 0
S4: 0

PDN-GW:

SGi: 0
S8B: 1
GX: 1
S6B: 0
S5: 1
S2C: 0
S2B: 0
S2A: 0

ENODEB:

UU: 0
X2: 1
S1-MME: 1

TCE IP Addr:

IPV4 Addr: 1.1.1.1

Hex: 6000 2200 2163 5400 3039 0000 0000 0000
003F 7040 0305 0000 0000 0000 0000 1F00
6803 0101 0101 335927



Troubleshooting the Service

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during service operation.

- [Test Commands](#), page 223

Test Commands

In the event that an issue was discovered with an installed application or line card, depending on the severity, it may be necessary to take corrective action.

The system provides several redundancy and fail-over mechanisms to address issues with application and line cards in order to minimize system downtime and data loss. These mechanisms are described in the sections that follow.

Using the PPP Echo-Test Command

The system provides a mechanism to verify the Point-to-Point Protocol session of a particular subscriber by sending Link Control Protocol (LCP) packets to the mobile node. This functionality can be extremely useful in determining the quality of the air link and delays that may occur.

The command has the following syntax:

ppp echo-test { **callid** *call_id* | **ipaddr** *ip_address* | **msid** *ms_id* | **username** *subscriber_name* }

Keyword/Variable	Description
callid <i>call_id</i>	Specifies that the test is executed for a subscriber with a specific call identification number (callid). <i>call_id</i> is the specific call identification number that you wish to test.
ipaddr <i>ip_address</i>	Specifies that the test is executed for a subscriber with a specific IP address. <i>ip_address</i> is the specific IP address that you wish to test.
msid <i>ms_id</i>	Specifies that the test is executed for a subscriber with a specific mobile station identification (MSID) number. <i>ms_id</i> is the specific mobile station identification number that you wish to test.

Keyword/Variable	Description
username <i>subscriber_name</i>	Specifies that the test is executed for a subscriber with a specific username. <i>subscriber_name</i> is the specific username that you wish to test.

The following figure displays a sample of this command's output showing a successful PPP echo-test to a subscriber named user2aaa.

```

USERNAME: user2aaa   MSID: 0000012345   CALLID: 001e8481
Tx/Rx 1/0   RTT (min/max/avg) 0/0/0
USERNAME: user2aaa   MSID: 0000012345   CALLID: 001e8481
Tx/Rx 1/1   RTT (min/max/avg) 77/77/77 (COMPLETE)

```

Using the GTPC Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-C echo request messages to the specified SGSN(s) and waiting for a response.



Important

This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpc test echo *src-address gn_address* { **all** | *sgsn-address ip_address* }

Keyword/Variable	Description
echo <i>src-address gn_address</i>	Specifies the IP address of a Gn interface configured on the system. Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address <i>ip_address</i>	Specifies that GTP-C echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN receiving the requests.

The following example displays a sample of this command's output showing a successful GTPC echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```

GTPC test echo
-----
SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 1 (COMPLETE) Recovery:202 (0xCA)

```

Using the GTPU Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-U echo request messages to the specified SGSN(s) and waiting for a response.

**Important**

This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpu test echo *src-address gn_address* { **all** | **sgsn-address** *ip_address* }

Keyword/Variable	Description
src-address <i>gn_address</i>	Specifies the IP address of a Gn interface configured on the system. Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTP-U echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address <i>ip_address</i>	Specifies that GTP-U echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN receiving the requests.

The following figure displays a sample of this command's output showing a successful GTPU echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPU test echo
-----
SGSN: 192.168.157.2   Tx/Rx:  1/1   RTT(ms): 24   (COMPLETE)
```

Using the GTPv0 Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTPv0 echo request messages to the specified SGSN(s) and waiting for a response.

**Important**

This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpv0 test echo *src-address gn_address* { **all** | **sgsn-address** *ip_address* }

Keyword/Variable	Description
src-address <i>gn_address</i>	Specifies the IP address of a Gn interface configured on the system. Important The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTPv0 echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address <i>ip_address</i>	Specifies that GTPv0 echo requests will be sent to a specific SGSN. <i>ip_address</i> is the address of the SGSN to receiving the requests.

The following figure displays a sample of this command's output showing a successful GTPv0 echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPv0 test echo
-----
SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms):14 (COMPLETE) Recovery: 210 (0xD2)
```

Using the DHCP Test Command

This command tests the system's ability to communicate with a Dynamic Host Control Protocol (DHCP) server. Testing is performed on a per-DHCP service basis for either a specific server or all servers the DHCP service is configured to communicate with. This functionality is useful for troubleshooting and/or monitoring.

Once executed, the test attempts to obtain an IP address from the DHCP server(s) and immediately release it.



Important This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

dhcp test dhcp-service *svc_name* [**all** | **server** *ip_address*]

Keyword/Variable	Description
dhcp-service <i>svc_name</i>	The name of the DHCP service. <i>svc_name</i> can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.
all	Tests DHCP functionality for all servers.
server <i>ip_address</i>	Tests DHCP functionality for the server.

The following figure displays a sample of this command's output showing a successful DHCP test for a DHCP service called DHCP-Gi to a server with an IP address of 192.168.16.2. The IP address provided during the test was 192.168.16.144.

```
DHCP test status for service <DHCP-Gi>:
  Server address: 192.168.16.2           Status: Tested
  Lease address: 192.168.16.144         Lease Duration: 600 secs.
```

Testing GTPP Accounting with a CGF

When used to test a CGF, this tool causes the system to send GTPP echo packets to the specified CGF(s).



Important This tool must be executed from the context in which GTPP functionality is configured.

To execute the GTPP accounting test tool enter the following command:

gtp test accounting { **all** | **cgf-server** *ip_address* }

Keyword/Variable	Description
all	Tests all CGFs configured within the given context.
cgf-server <i>ip_address</i>	Tests a specific CGF configured within the given context.

The command's response will display whether the CGF is active or unreachable.

Testing GTPP Connectivity with a GSS

When used to test a GTPP Storage Server, this tool causes the system to send GTPP echo packets to the specified GSS for checking connectivity and provide round trip time.



Important This tool must be executed from the context in which GTPP functionality is configured.

To execute the GSS connectivity test tool enter the following command:

gtp test storage-server [**address** *ip-address* **port** *udp-port*]

Keyword/Variable	Description
storage-server	Tests configured GSS within the given context.
address <i>ip_address</i> port <i>udp_port</i>	Tests connectivity with GSS having <i>ip_address</i> and <i>udp_port</i> before configuring it within the given context.

The command's response will display whether the GSS is active or unreachable.



3GPP ULI Reporting Support Enhanced

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

- [Feature Change, page 229](#)

Feature Change

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Action towards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)

Event Trigger from PCRF	MS Info Change Reporting Action towards SGSN
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

Behavior Change

Previous of Change Reporting Action: Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

Behavior of MS Info Change Reporting Action: Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

Limitations

- 1 In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
- 2 In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.



CHAPTER 11

Backup and Recovery of Key KPI Statistics

This feature allows the backup of GGSN, P-GW, SAEGW, and/or S-GW counters for recovery of key KPI counter values after a session manager (SessMgr) restart.

This chapter includes the following information:

- [Feature Description, page 231](#)
- [How It Works, page 231](#)
- [Configuring Backup Statistics Feature, page 233](#)

Feature Description

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

How It Works

A key set of counters used in KPI computation will be backed up for recovery if a SessMgr task restarts. The counters that will be backed up are determined by the KPIs typically used in several operator networks.

The backup of counters is enabled or disabled via configuration. The configuration specifies the product (GGSN, P-GW, SAEGW, and/or S-GW) for which counters will be backed up and also a time interval for the backup of the counters.

Architecture

When this feature is enabled (see *Configuring Backup Statistics Feature* below), the GGSN, P-GW, SAEGW, and/or S-GW only backs up the counters maintained at the SessMgr. The recovery function does not need to be configured or started as it occurs automatically as needed when the feature is enabled.

The counters are backed up to the AAAMgr that is paired with the SessMgr.

Checkpointing

Node-level statistics are checkpointed at AAAMgr. Once statistics are backed up for a specific product, all the associated services, such as eGTP-C and GTP-U statistics, are also checkpointed.

Recovery

When SessMgr restarts, recovery is performed by receiving all the stored statistics from the mapped AAAMgr and the recovered values are added to the backup counters maintained at per-service level. This will not impact session recovery time as the backed up counters are pushed to SessMgr only after session recovery is complete.

Since session recovery is complete, the session managers may start processing calls. In such cases, the counters will continue to be incremented. The recovered values of the corresponding counters will always be added to the existing counters. Gauge counters are checkpointed but not recovered.

Order of Statistics Collection

The upper limit of checkpoint messaging is a maximum of 1 MB. Before picking any node to checkpoint, available memory is checked. If memory is insufficient, the whole node is discarded.

Since there is 1 MB limit, nodes/statistics to checkpoint are prioritized as follows:

- 1 SAEGW statistics:
 - P-GW and S-GW service node-level statistics collected
- 2 P-GW service node configuration will store the following statistics:
 - P-GW, eGTP-C ingress, GTP-U ingress, per-interface (s2a, s2b, s5s8), and GGSN (if associated) statistics collected
 - SAEGW associated P-GW service statistics not collected
- 3 S-GW service node configuration will store the following statistics:
 - S-GW, eGTP-C ingress/egress, and GTP-U ingress/egress statistics collected
 - SAEGW associated S-GW service statistics not collected
- 4 GGSN statistics:
 - GGSN service statistics, if not associated with P-GW service, collected
- 5 Session disconnect reasons collected if GGSN/P-GW/SAEGW/S-GW is enabled

Error Handling

If adding new statistics is going to cause overflow of 1 MB buffer, that service and the corresponding node will not be included. Checkpointing of any further nodes will also be stopped. Error level log will be flagged if total memory requirement goes above 1 MB.

Limitations

- A backup interval must be specified and counters are backed up only at the specified interval. For example, if the backup interval is specified as 5 minutes, then counters are backed up every 5 minutes. Suppose backup happened at Nth minute and the configured backup interval is for every 5 minutes, then if a task crash happens at N+4 minutes, the GGSN, P-GW, SAEGW, and/or S-GW recovers only the values backed up at Nth minute and the data for the past 4 minutes is lost.
- Only statistics maintained at the SessMgr are backed up. Statistics at other managers are not backed up or recovered.
- The following statistics are not considered for backup:
 - APN-level statistics
 - eGTP-C APN-QCI statistics
 - DemuxMgr statistics
- The CLI command **clear statistics** will not trigger checkpoint to delete the node statistics on AAAMgr. New checkpoint after timer expiry will overwrite the statistics.
- Maximum of 1 MB of statistics will be stored on AAAMgr. Services after the maximum size limit are not backed up.
- Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.
- If SessMgr restarts and AAAMgr restarts before SessMgr recovers statistics from AAAMgr, then backed up statistics are lost.
- This feature is not applicable for ICSR.

Configuring Backup Statistics Feature

For the Backup and Recovery of Key KPI Statistics feature to work, it must be enabled by configuring the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

Configuration

The following CLI commands are used to manage the functionality for the backing up of the key KPI statistics feature.

Enabling

The following configures the backup of statistics for the GGSN, P-GW, SAEGW, and/or S-GW and enables the Backup and Recovery of Key KPI Statistics feature.

```
configure
  statistics-backup { ggsn | pgw | saegw | sgw }
```

```
exit
```

Setting the Backup Interval

The following command configures the number of minutes (0 to 60) between each backup of the statistics. When the backup interval is not specified, a default value of 5 minutes is used as the backup interval

```
configure
  statistics-backup-interval minutes
exit
```



Important

Setting the backup interval to shorter periods of time causes higher system overhead for checkpointing. Alternately, setting the backup interval to longer periods of time results in lower system overhead for checkpointing but higher probability of hitting the 1 MB storage limit.

Disabling

The following configures the GGSN, P-GW, SAEGW, and/or S-GW to disable the backing up of statistics for the GGSN, P-GW, SAEGW, and/or S-GW.

```
configure
  no statistics-backup { ggsn | pgw | saegw | sgw }
exit
```

Verifying the Backup Statistics Feature Configuration

Use either the **show configuration** command or the **show configuration verbose** command to display the feature configuration.

If the feature was enabled in the configuration, two lines similar to the following will appear in the output of a **show configuration [verbose]** command:

```
statistics-backup pgw
statistics-backup-interval 5
```

Notes:

- The interval displayed is 5 minutes. 5 is the default. If the **statistics-backup-interval** command is included in the configuration, then the 5 would be replaced by the configured interval number of minutes.
- If the command to disable the feature is entered, then no **statistics-backup** line is displayed in the output generated by a **show configuration [verbose]** command.



Bulkstats for Average Data Rate per IPP00L

- [Feature Summary and Revision History, page 235](#)
- [Feature Description, page 236](#)
- [Monitoring and Troubleshooting, page 236](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	<ul style="list-style-type: none">• GGSN• P-GW
Applicable Platform(s)	<ul style="list-style-type: none">• ASR 5500• VPC - DI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	<i>Statistics and Counters Reference</i>

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

In this enhancement, bulkstat support has been added for fetching subscriber average data-rate per IP pool (cumulative of all sessmgr) for all the IP pools configured in the system.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands and bulk statistics available to support of this feature.

Bulk Statistics

The following bulk stats have been added to the respective schemas as part of this feature:

Datarate-IPPool Schema

The following bulk statistics are added to the Datarate-IPPool Schema:

- sess-datarate-ippool-name - Indicates name of the ip pool for which average data rates are fetched.
- sess-ave-rate-fuser-bps - indicates average data-rate(bits/sec) from user in uplink direction per ip pool basis.
- sess-ave-rate-tuser-bps - indicates average data-rate(bits/sec) to user in downlink direction per ip pool basis.
- sess-ave-rate-fuser-pps - indicates average packets/sec from user in uplink direction per ip pool basis.
- sess-ave-rate-tuser-pps - indicates average packets/sec to user in downlink direction per ip pool basis.

Show Commands and/or Outputs

This section provides information regarding show commands and their outputs for this feature.

show bulkstats schemas

This command has been modified to display the following output:

```
Bulk Statistics Server Configuration:
  Server State:           Enabled
  File Limit:             7500 KB
  Sample Interval:        10 minutes (0D 0H 10M)
  Transfer Interval:      15 minutes (0D 0H 15M)
  Receiver Mode:          Secondary-on-failure
  .....
  .....
----- Schemas for File 1 -----
Type      Name              Active-Only  Format
-----
datarate-ippool datarate_ippool1      No
```



```
EMS,datarate_ippool1,%date%,%time%,%sess-datarate-ippool-name%,%sess-ave-rate-fuser-bps%,%sess-ave-rate-tuser-bps%,%sess-ave-rate-fuser-pps%,%sess-ave-rate-tuser-pps%
```

show bulkstats data

This command has been modified to display the Bulk Statistics Server Configuration:

```
Server State:                Enabled
File Limit:                  7500 KB
Sample Interval:             10 minutes (0D 0H 10M)
Transfer Interval:           15 minutes (0D 0H 15M)
Receiver Mode:               Secondary-on-failure
.....
Pending Data for File 1:
-----
EMS,datarate_ippool1,20170619,211715,pp2,455,455,1,1
```

show subscribers data-rate ip-pool <pool_name>

This command has been modified to display the following output:

Total Subscribers	: 1		
Active	: 1	Dormant	: 0
peak rate from user(bps):	672	peak rate to user(bps)	: 672
ave rate from user(bps) :	455	ave rate to user(bps)	: 455
sust rate from user(bps):	455	sust rate to user(bps)	: 455
peak rate from user(pps):	1	peak rate to user(pps)	: 1
ave rate from user(pps) :	1	ave rate to user(pps)	: 1
sust rate from user(pps):	0	sust rate to user(pps)	: 0



CoA, RADIUS DM, and Session Redirection (Hotlining)

This chapter describes Change of Authorization (CoA), Disconnect Message (DM), and Session Redirect (Hotlining) support in the system. RADIUS attributes, Access Control Lists (ACLs) and filters that are used to implement these features are discussed. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in this Administration Guide, before using the procedures in this chapter.



Important

Not all functions, commands, and keywords/variables are available or supported for all network function or services. This depends on the platform type and the installed license(s).

- [RADIUS Change of Authorization and Disconnect Message](#), page 239
- [Session Redirection \(Hotlining\)](#), page 244

RADIUS Change of Authorization and Disconnect Message

This section describes how the system implements CoA and DM RADIUS messages and how to configure the system to use and respond to CoA and DM messages.

CoA Overview

The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session. The filter-id attribute (attribute ID 11) contains the name of an Access Control List (ACL). For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*.

If the system successfully executes a CoA request, a CoA-ACK message is sent back to the RADIUS server and the data filter is applied to the subscriber session. Otherwise, a CoA-NAK message is sent with an error-cause attribute without making any changes to the subscriber session.

**Important**

Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

DM Overview

The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session. If the system successfully disconnects the subscriber session, a DM-ACK message is sent back to the RADIUS server, otherwise, a DM-NAK message is sent with proper error reasons.

License Requirements

The RADIUS Change of Authorization (CoA) and Disconnect Message (DM) are licensed Cisco features. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Enabling CoA and DM

To enable RADIUS Change of Authorization and Disconnect Message:

-
- Step 1** Enable the system to listen for and respond to CoA and DM messages from the RADIUS server as described in [Enabling CoA and DM, on page 240](#).
- Step 2** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 3** View CoA and DM message statistics as described in [Viewing CoA and DM Statistics, on page 243](#).
- Important** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands. Not all commands and keywords/variables are available or supported. This depends on the platform type and the installed license(s).
-

Enabling CoA and DM

Use the following example to enable the system to listen for and respond to CoA and DM messages from the RADIUS server:

```
configure
context <context_name>
```

```
radius change-authorize-nas-ip <ipv4/ipv6_address>
end
```

Notes:

- `<context_name>` must be the name of the AAA context where you want to enable CoA and DM.
For more information on configuring the AAA context, if you are using StarOS 12.3 or an earlier release, refer to the *Configuring Context-Level AAA Functionality* section of the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.
- A number of optional keywords and variables are available for the **radius change-authorize-nas-ip** command. For more information regarding this command please refer to the *Command Line Interface Reference*.

CoA and DM Attributes

For CoA and DM messages to be accepted and acted upon, the system and subscriber session to be affected must be identified correctly.

To identify the system, use any one of the following attributes:

- NAS-IP-Address: NAS IP address if present in the CoA/DM request should match with the NAS IP address.
- NAS-Identifier: If this attribute is present, its value should match to the nas-identifier generated for the subscriber session

To identify the subscriber session, use any one of the following attributes.

- If 3GPP2 service is configured the following attribute is used for correlation identifier:
 - 3GPP2-Correlation-ID: The values should exactly match the 3GPP2-correlation-id of the subscriber session. This is one of the preferred methods of subscriber session identification.
- If 3GPP service is configured the following attributes are used for different identifiers:
 - 3GPP-IMSI: International Mobile Subscriber Identification (IMSI) number should be validated and matched with the specified IMSI for specific PDP context.
 - 3GPP-NSAPI: Network Service Access Point Identifier (NSAPI) should match to the NSAPI specified for specific PDP context.
- User-Name: The value should exactly match the subscriber name of the session. This is one of the preferred methods of subscriber session identification.
- Framed-IP-Address: The values should exactly match the framed IP address of the session.
- Calling-station-id: The value should match the Mobile Station ID.

To specify the ACL to apply to the subscriber session, use the following attribute:

- Filter-ID: CoA only. This must be the name of an existing Access Control List. If this is present in a CoA request, the specified ACL is immediately applied to the specified subscriber session. The Context Configuration mode command, **radius attribute filter-id direction**, controls in which direction filters are applied.

The following attributes are also supported:

- Event-Timestamp: This attribute is a timestamp of when the event being logged occurred.
- If 3GPP2 service is configured following additional attributes are supported:
 - 3GPP2-Disconnect-Reason: This attribute indicates the reason for disconnecting the user. This attribute may be present in the RADIUS Disconnect-request Message from the Home Radius server to the PDSN.
 - 3GPP2-Session-Termination-Capability: When CoA and DM are enabled by issuing the radius change-authorize-nas-ip command, this attribute is included in a RADIUS Access-request message to the Home RADIUS server and contains the value 3 to indicate that the system supports both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute is also included in the RADIUS Access-Accept message and contains the preferred resource management mechanism by the home network, which is used for the session and may include values 1 through 3.

CoA and DM Error-Cause Attribute

The Error-Cause attribute is used to convey the results of requests to the system. This attribute is present when a CoA or DM NAK or ACK message is sent back to the RADIUS server.

The value classes of error causes are as follows:

- 0-199, 300-399 reserved
- 200-299 - successful completion
- 400-499 - errors in RADIUS server
- 500-599 - errors in NAS/Proxy

The following error cause is sent in ACK messages upon successful completion of a CoA or DM request:

- 201- Residual Session Context Removed

The following error causes are sent in NAK messages when a CoA or DM request fails:

- 401 - Unsupported Attribute
- 402 - Missing Attribute
- 403 - NAS Identification Mismatch
- 404 - Invalid Request
- 405 - Unsupported Service
- 406 - Unsupported Extension
- 501 - Administratively Prohibited
- 503 - Session Context Not Found
- 504 - Session Context Not Removable
- 506 - Resources Unavailable

Viewing CoA and DM Statistics

View CoA and DM message statistics by entering the following command:

show session subsystem facility aaamgr

The following is a sample output of this command.

```

1 AAA Managers
807 Total aaa requests
379 Total aaa auth requests
    0 Total aaa auth probes
    0 Total aaa auth keepalive
426 Total aaa acct requests
    0 Total aaa acct keepalive
379 Total aaa auth success
    0 Total aaa auth purged
    0 Total auth keepalive success
    0 Total auth keepalive purged
    0 Total aaa auth DMU challenged
367 Total radius auth requests
    2 Total radius auth requests retried
    0 Total radius auth responses dropped
    0 Total local auth requests
12 Total pseudo auth requests
    0 Total null-username auth requests (rejected)
    0 Total aaa acct completed
    0 Total acct keepalive success
    0 Total acct keepalive purged
    0 Total aaa acct cancelled
426 Total radius acct requests
    0 Total radius acct requests retried
    0 Total radius acct responses dropped
    0 Total gtpa acct requests
    0 Total gtpa acct cancelled
    0 Total null acct requests
54 Total aaa acct sessions
    3 Total aaa acct archived
    0 Current recovery archives

    2 Total aaa sockets opened
    0 Total aaa requests pend socket open
    0 Current aaa requests pend socket open
    0 Total radius requests pend server max-outstanding
    0 Current radius requests pend server max-outstanding
    0 Total aaa radius coa requests
    0 Total aaa radius coa acks
    0 Total aaa radius coa naks
    2 Total radius charg auth
    0 Total radius charg auth succ
    0 Total radius charg auth purg

    0 Total radius charg acct
    0 Total radius charg acct succ
    0 Total radius charg acct cancel
357 Total gtpa charg
357 Total gtpa charg success
    0 Total gtpa charg cancel
    0 Total prepaid online requests

    0 Total prepaid online success

    0 Total prepaid online retried

    0 Current prepaid online purged
    0 Total aaamgr purged requests
    0 SGSN: Total db records
    0 SGSN: Total sub db records
    0 SGSN: Total mm records
    0 SGSN: Total pdp records
    0 SGSN: Total auth records
0 Current aaa requests
0 Current aaa auth requests
0 Current aaa auth probes
0 Current aaa auth keepalive
0 Current aaa acct requests
0 Current aaa acct keepalive
0 Total aaa auth failure
0 Total aaa auth cancelled
0 Total auth keepalive failure
0 Current radius auth requests
0 Current local auth requests
0 Current pseudo auth requests
0 Total aaa acct purged
0 Total acct keepalive timeout
0 Current radius acct requests
0 Current gtpa acct requests
0 Total gtpa acct purged
0 Current null acct requests
5 Current aaa acct sessions
0 Current aaa acct archived
0 Current valid recovery records
2 Current aaa sockets open
0 Total aaa radius dm requests
0 Total aaa radius dm acks
0 Total aaa radius dm naks
0 Current radius charg auth
0 Total radius charg auth fail
0 Total radius charg auth cancel
0 Current radius charg acct
0 Total radius charg acct purg
0 Current gtpa charg
0 Total gtpa charg failure
0 Total gtpa charg purg
0 Current prepaid online requests
0 Current prepaid online failure
0 Total prepaid online cancelled

```

Session Redirection (Hotlining)

**Important**

Functionality described for this feature in this segment is not applicable for HNB-GW sessions.

Overview

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address. Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the RADIUS Change of Authorization (CoA) feature.

Note that the session redirection feature is only intended to redirect a very small subset of subscribers at any given time. The data structures allocated for this feature are kept to the minimum to avoid large memory overhead in the session managers.

License Requirements

The Session Redirection (Hotlining) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Operation

ACL Rule

An ACL rule named **readdress server** supports redirection of subscriber sessions. The ACL containing this rule must be configured in the destination context of the user. Only TCP and UDP protocol packets are supported. The ACL rule allows specifying the redirected address and an optional port. The source and destination address and ports (with respect to the traffic originating from the subscriber) may be wildcarded. If the redirected port is not specified, the traffic will be redirected to the same port as the original destination port in the datagrams. For detailed information on configuring ACLs, refer to the *IP Access Control Lists* chapter in the *System Administration Guide*. For more information on **readdress server**, refer to the *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Redirecting Subscriber Sessions

An ACL with the **readdress server** rule is applied to an existing subscriber session through CoA messages from the RADIUS server. The CoA message contains the 3GPP2-Correlation-ID, User-Name, Acct-Session-ID, or Framed-IP-Address attributes to identify the subscriber session. The CoA message also contains the Filter-Id attribute which specifies the name of the ACL with the **readdress server** rule. This enables applying the ACL

dynamically to existing subscriber sessions. By default, the ACL is applied as both the input and output filter for the matching subscriber unless the Filter-Id in the CoA message bears the prefix **in:** or **out:**.

For information on CoA messages and how they are implemented in the system, refer to [RADIUS Change of Authorization and Disconnect Message](#), on page 239.

**Important**

Changing ACL and rulebase together in a single CoA is not supported. For this, two separate CoA requests can be sent through AAA server requesting for one attribute change per request.

Session Limits On Redirection

To limit the amount of memory consumed by a session manager a limit of 2000 redirected session entries per session manager is allocated. This limit is equally shared by the set of subscribers who are currently being redirected. Whenever a redirected session entry is subject to revocation from a subscriber due to an insufficient number of available session entries, the least recently used entry is revoked.

Stopping Redirection

The redirected session entries for a subscriber remain active until a CoA message issued from the RADIUS server specifies a filter that does not contain the readdress server ACL rule. When this happens, the redirected session entries for the subscriber are deleted.

All redirected session entries are also deleted when the subscriber disconnects.

Handling IP Fragments

Since TCP/UDP port numbers are part of the redirection mechanism, fragmented IP datagrams must be reassembled before being redirected. Reassembly is particularly necessary when fragments are sent out of order. The session manager performs reassembly of datagrams and reassembly is attempted only when a datagram matches the redirect server ACL rule. To limit memory usage, only up to 10 different datagrams may be concurrently reassembled for a subscriber. Any additional requests cause the oldest datagram being reassembled to be discarded. The reassembly timeout is set to 2 seconds. In addition, the limit on the total number of fragments being reassembled by a session manager is set to 1000. If this limit is reached, the oldest datagram being reassembled in the session manager and its fragment list are discarded. These limits are not configurable.

Recovery

When a session manager dies, the ACL rules are recovered. The session redirect entries have to be re-created when the MN initiates new traffic for the session. Therefore when a crash occurs, traffic from the Internet side is not redirected to the MN.

AAA Accounting

Where destination-based accounting is implemented, traffic from the subscriber is accounted for using the original destination address and not the redirected address.

Viewing the Redirected Session Entries for a Subscriber

View the redirected session entries for a subscriber by entering the following command:

show subscribers debug-info { callid <id> | msid <id> | username <name> }

The following command displays debug information for a subscriber with the MSID 0000012345:

show subscribers debug-info msid 0000012345

The following is a sample output of this command:

```
username: user1 callid: 01callb1      msid: 0000100003
Card/Cpu: 4/2
Sessmgr Instance: 7
Primary callline:
Redundancy Status: Original Session
Checkpoints  Attempts  Success  Last-Attempt  Last-Success
Full:        27       26       15700ms      15700ms
Micro:       76       76       4200ms       4200ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
      State                               Event
      SMGR_STATE_OPEN                    SMGR_EVT_NEWCALL
      SMGR_STATE_NEWCALL_ARRIVED          SMGR_EVT_ANSWER_CALL
      SMGR_STATE_NEWCALL_ANSWERED         SMGR_EVT_LINE_CONNECTED
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_LINK_CONTROL_UP
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_AUTH_REQ
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_IPADDR_ALLOC_SUCCESS
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_AUTH_SUCCESS
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_UPDATE_SESS_CONFIG
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_LOWER_LAYER_UP

Data Reorder statistics
      Total timer expiry: 0               Total flush (tmr expiry): 0
      Total no buffers: 0                 Total flush (no buffers): 0
      Total flush (queue full): 0         Total flush (out of range): 0
      Total flush (svc change): 0         Total out-of-seq pkt drop: 0
      Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:
      Success: 0                         In Progress: 0
      Failure (timeout): 0               Failure (no buffers): 0
      Failure (other reasons): 0

Redirected Session Entries:
      Allowed: 2000                      Current: 0
      Added: 0                          Deleted: 0
      Revoked for use by different subscriber: 0

Peer callline:
Redundancy Status: Original Session
Checkpoints  Attempts  Success  Last-Attempt  Last-Success
Full:        0        0        0ms            0ms
Micro:       0        0        0ms            0ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
      State                               Event
      SMGR_STATE_OPEN                    SMGR_EVT_MAKECALL
      SMGR_STATE_MAKECALL_PENDING         SMGR_EVT_LINE_CONNECTED
      SMGR_STATE_LINE_CONNECTED           SMGR_EVT_LOWER_LAYER_UP
      SMGR_STATE_CONNECTED                 SMGR_EVT_AUTH_REQ
      SMGR_STATE_CONNECTED                 SMGR_EVT_AUTH_SUCCESS
      SMGR_STATE_CONNECTED                 SMGR_EVT_REQ_SUB_SESSION
      SMGR_STATE_CONNECTED                 SMGR_EVT_RSP_SUB_SESSION

username: user1 callid: 01callb1      msid: 0000100003
Card/Cpu: 4/2
Sessmgr Instance: 7
Primary callline:
Redundancy Status: Original Session
Checkpoints  Attempts  Success  Last-Attempt  Last-Success
Full:        27       26       15700ms      15700ms
Micro:       76       76       4200ms       4200ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
      State                               Event
```

```

SMGR_STATE_OPEN                      SMGR_EVT_NEWCALL
SMGR_STATE_NEWCALL_ARRIVED          SMGR_EVT_ANSWER_CALL
SMGR_STATE_NEWCALL_ANSWERED         SMGR_EVT_LINE_CONNECTED
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_LINK_CONTROL_UP
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_AUTH_REQ
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_IPADDR_ALLOC_SUCCESS
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_AUTH_SUCCESS
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_UPDATE_SESS_CONFIG
SMGR_STATE_LINE_CONNECTED            SMGR_EVT_LOWER_LAYER_UP

Data Reorder statistics
  Total timer expiry: 0               Total flush (tmr expiry): 0
  Total no buffers: 0                 Total flush (no buffers): 0
  Total flush (queue full): 0         Total flush (out of range): 0
  Total flush (svc change): 0         Total out-of-seq pkt drop: 0
  Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:
  Success: 0                         In Progress: 0
  Failure (timeout): 0               Failure (no buffers): 0
  Failure (other reasons): 0

Redirected Session Entries:
  Allowed: 2000                      Current: 0
  Added: 0                           Deleted: 0
  Revoked for use by different subscriber: 0

Peer callline:
Redundancy Status: Original Session
Checkpoints  Attempts  Success  Last-Attempt  Last-Success
Full:        0         0         0ms           0ms
Micro:       0         0         0ms           0ms
Current state: SMGR_STATE_CONNECTED
FSM Event trace:
  State                      Event
  SMGR_STATE_OPEN           SMGR_EVT_MAKECALL
  SMGR_STATE_MAKECALL_PENDING SMGR_EVT_LINE_CONNECTED
  SMGR_STATE_LINE_CONNECTED  SMGR_EVT_LOWER_LAYER_UP
  SMGR_STATE_CONNECTED       SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED       SMGR_EVT_AUTH_SUCCESS
  SMGR_STATE_CONNECTED       SMGR_EVT_REQ_SUB_SESSION
  SMGR_STATE_CONNECTED       SMGR_EVT_RSP_SUB_SESSION
  SMGR_STATE_CONNECTED       SMGR_EVT_ADD_SUB_SESSION
  SMGR_STATE_CONNECTED       SMGR_EVT_AUTH_REQ
  SMGR_STATE_CONNECTED       SMGR_EVT_AUTH_SUCCESS

Data Reorder statistics
  Total timer expiry: 0               Total flush (tmr expiry): 0
  Total no buffers: 0                 Total flush (no buffers): 0
  Total flush (queue full): 0         Total flush (out of range): 0
  Total flush (svc change): 0         Total out-of-seq pkt drop: 0
  Total out-of-seq arrived: 0

IPv4 Reassembly Statistics:
  Success: 0                         In Progress: 0
  Failure (timeout): 0               Failure (no buffers): 0
  Failure (other reasons): 0

Redirected Session Entries:
  Allowed: 2000                      Current: 0
  Added: 0                           Deleted: 0
  Revoked for use by different subscriber: 0

```




Direct Tunnel for 4G (LTE) Networks

This chapter briefly describes support for direct tunnel (DT) functionality over an S12 interface for a 4G (LTE) network to optimize packet data traffic.

Cisco LTE devices (per 3GPP TS 23.401 v8.3.0) supporting direct tunnel include:

- Serving GPRS Support Node (S4-SGSN)
- Serving Gateway (S-GW)
- PDN Gateway (P-GW)



Important

Direct Tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The following sections are included in this chapter:

- [Direct Tunnel for 4G Networks - Feature Description](#) , page 249
- [How It Works](#), page 252
- [Configuring Support for Direct Tunnel](#), page 280
- [Monitoring and Troubleshooting Direct Tunnel](#), page 283

Direct Tunnel for 4G Networks - Feature Description

The amount of user plane data will increase significantly during the next few years because of High Speed Packet Access (HSPA) and IP Multimedia Subsystem technologies. Direct tunneling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates.

Direct Tunnel (DT) offers a solution that optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

Important

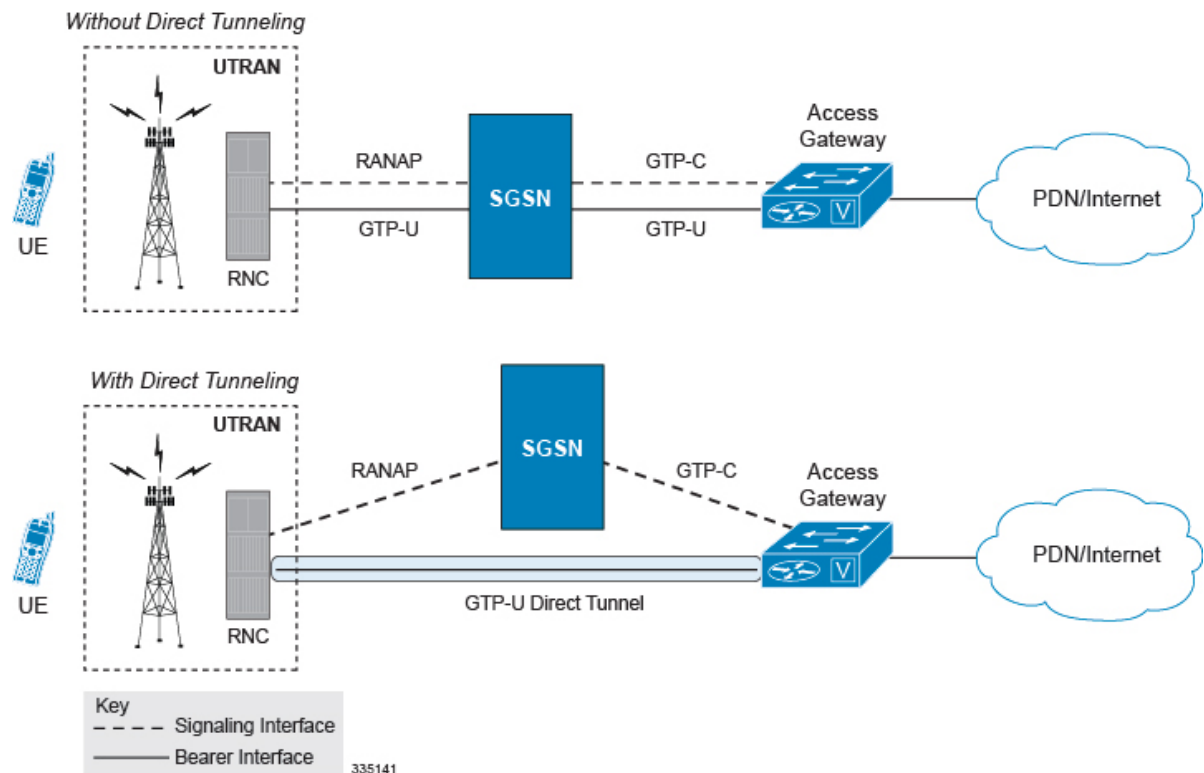
Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important

Establishment of a direct tunnel is controlled by the SGSN; for 4G networks this requires an S4 license-enabled SGSN setup and configured as an S4-SGSN.

Once a direct tunnel is established, the S4-SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

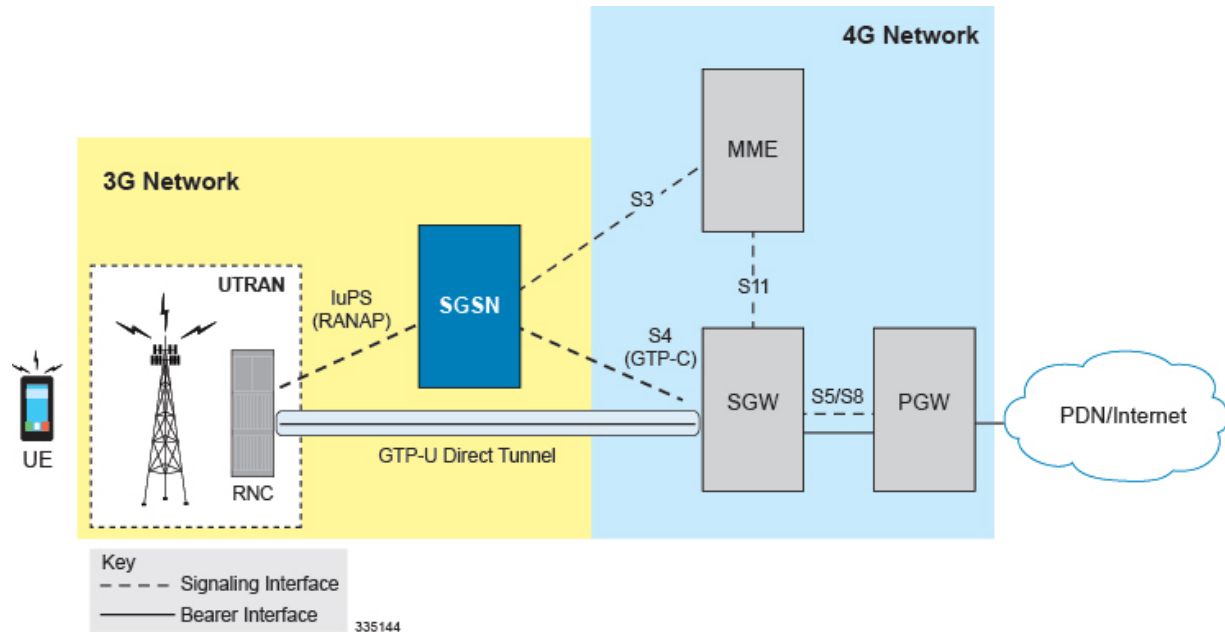
Figure 35: GTP-U Direct Tunneling



A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the S4-SGSN/S-GW to handle the user plane processing.

A direct tunnel is achieved upon PDP context activation when the S4-SGSN establishes a user plane tunnel (GTP-U tunnel) directly between the RNC and the S-GW over an S12 interface, using a Create Bearer Response or Modify Bearer Request towards the S-GW.

Figure 36: Direct Tunneling - LTE Network, S12 Interface



A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

S4-SGSN supports establishment of a GTP-U direct tunnel between an RNC and the S-GW under the scenarios listed below:

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without S-GW change
- Intra SGSN Routing Area Update with S-GW change
- Intra SGSN SRNS relocation without S-GW change
- Intra SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation without S-GW relocation
- E-UTRAN-to-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well

- UTRAN-to-E-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- Network Initiated PDP Activation

Scenarios that vary at S4-SGSN when direct tunneling is enabled, as compared to DT on a 2G or 3G SGSN using the Gn interface, include:

- RAB Release
- Iu Release
- Error Indication from RNC
- Downlink Data Notification from S-GW
- Downlink Data Error Indication from S-GW
- MS Initiated PDP Modification
- P-GW Initiated PDP Modification while the UE is IDLE
- HLR/HSS Initiated PDP Modification
- Session Recovery with Direct Tunnel

The above scenarios exhibit procedural differences in S4-SGSN when a direct tunnel is established.

How It Works

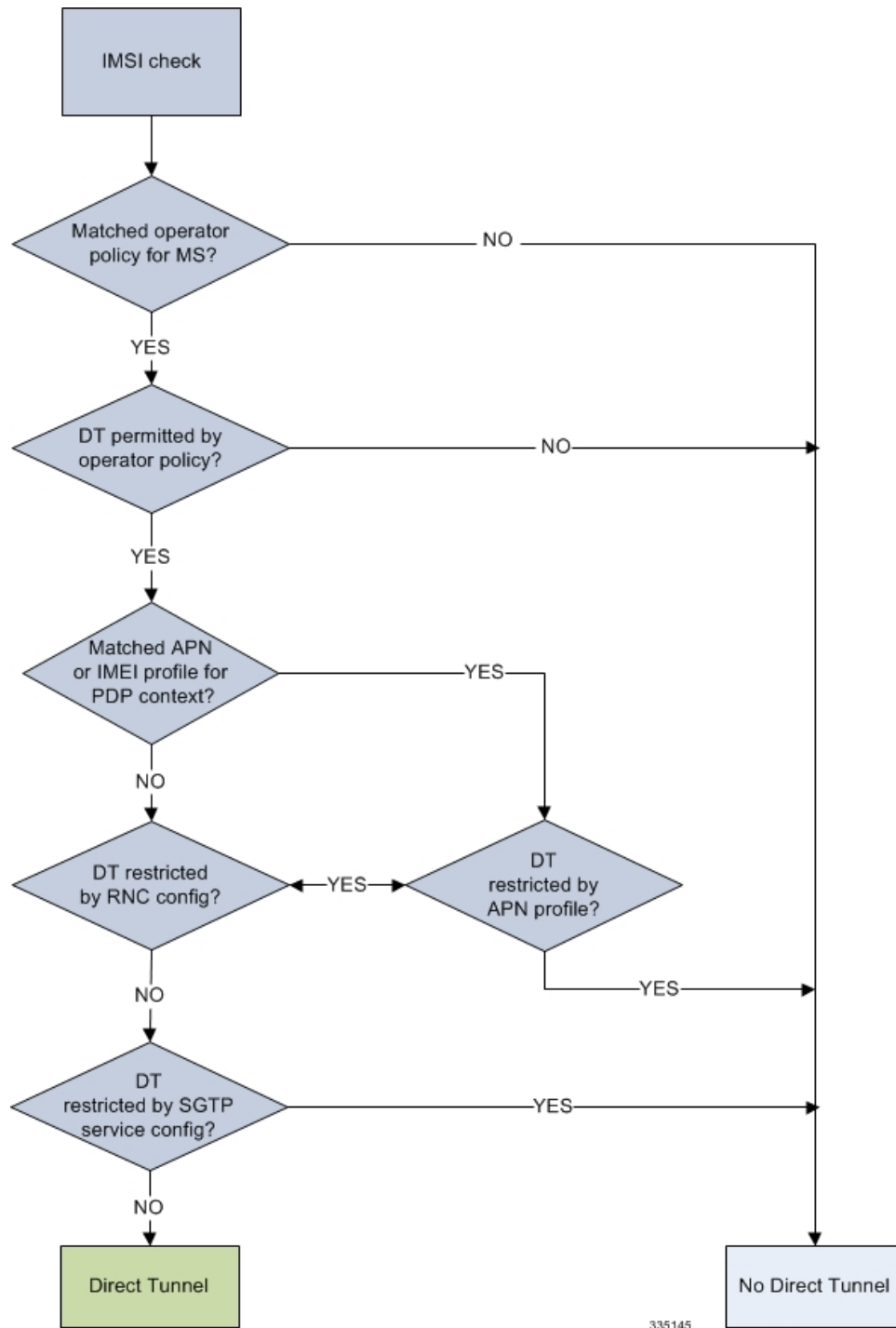
DT functionality enables direct user plane tunnel between RNC and SGW within the PS domain. With direct tunneling the S4-SGSN provides the RNC with the TEID and user plane address of the S-GW, and also provides the S-GW with the TEID and user plane address of the RNC.

The SGSN handles the control plane signaling and makes the decision when to establish the direct tunnel between RNC and S-GW, or use two tunnels for this purpose (based on configuration).

DT Establishment Logic

The following figure illustrates the logic used within the S4-SGSN/S-GW to determine if a direct tunnel will be setup.

Figure 37: Direct Tunneling - Establishment Logic



Establishment of Direct Tunnel

The S4-SGSN uses the S12 interface for DT.

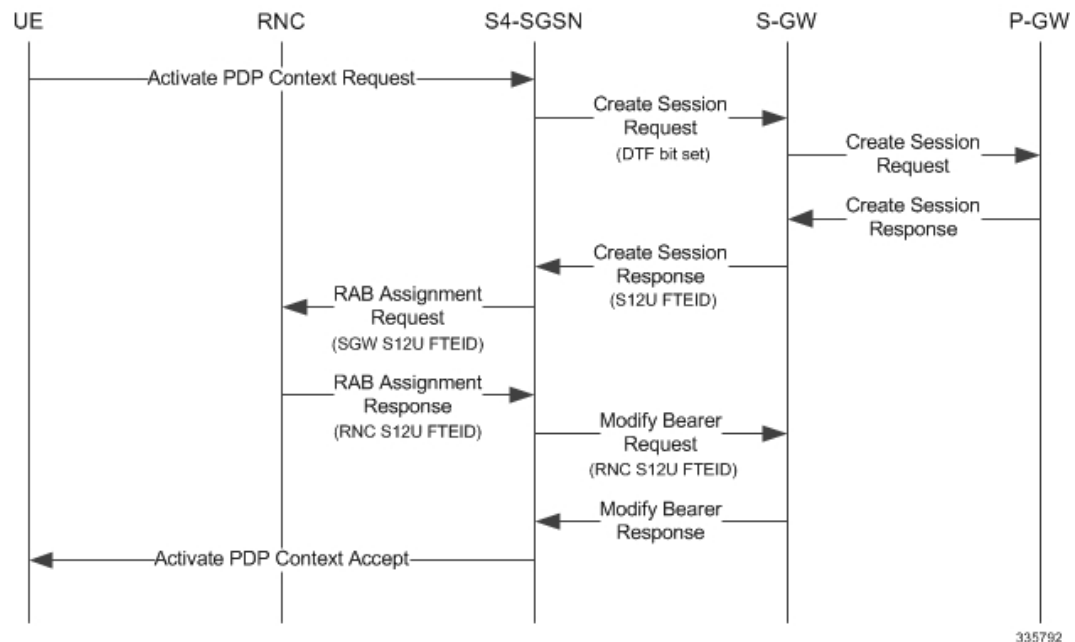
Direct Tunnel Activation for Primary PDP Context

For the PDP Context Activation procedure this solution uses new information elements (IEs) for the GPRS Tunnelling Protocol v2 (GTPv2) as defined in TS 29.274. SGSN provides the user plane addresses for RNC and S-GW as S12U FTEIDs as illustrated in the figure below.

The sequence for establishing a direct tunnel between the RNC and S-GW during PDP activation is as follows:

- SGSN sends a Create Session Request to the S-GW with the indication flag DTF (direct tunnel flag) bit set
- In its Create Session Response, the S-GW sends the SGSN an S12U FTEID (Fully Qualified Tunnel Endpoint Identifier).
- The SGSN forwards the S-GW S12U to the RNC during the RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends the SGSN its transport address and Tunnel Endpoint ID (TEID).
- The SGSN forward the RNC S12 U FTEID o the S-GW via a Modify Bearer Request.

Figure 38: Primary PDP Activation with Direct Tunnel



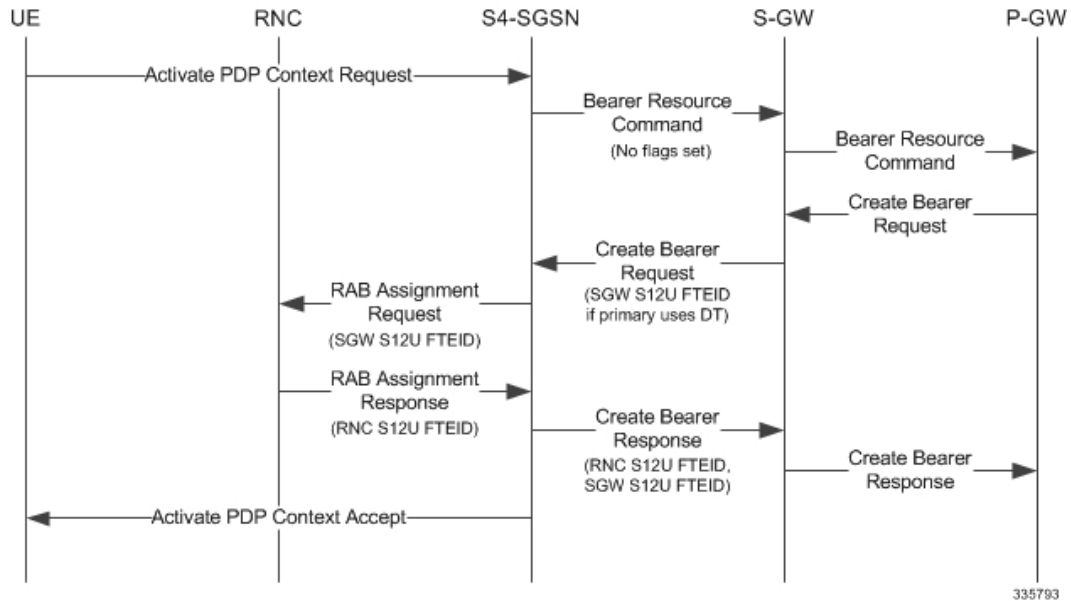
Direct Tunnel Activation for UE Initiated Secondary PDP Context

The following is the general sequence for establishing a direct tunnel for a Secondary PDP Context Activation:

- The SGSN sends a Bearer Resource Command to the S-GW with no flags set. (S-GW already knows Direct Tunnel is enabled for primary.)
- The S-GW sends a Create Bearer Response that includes the S12U FTEID to the SGSN.

- The SGSN forwards the S-GW S12U to RNC via a RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends its transport address and TEID to the SGSN.
- The SGSN forwards the S12U TEID received from the RNC to the S-GW via a Create Bearer Response.

Figure 39: Secondary PDP Activation with Direct Tunnel



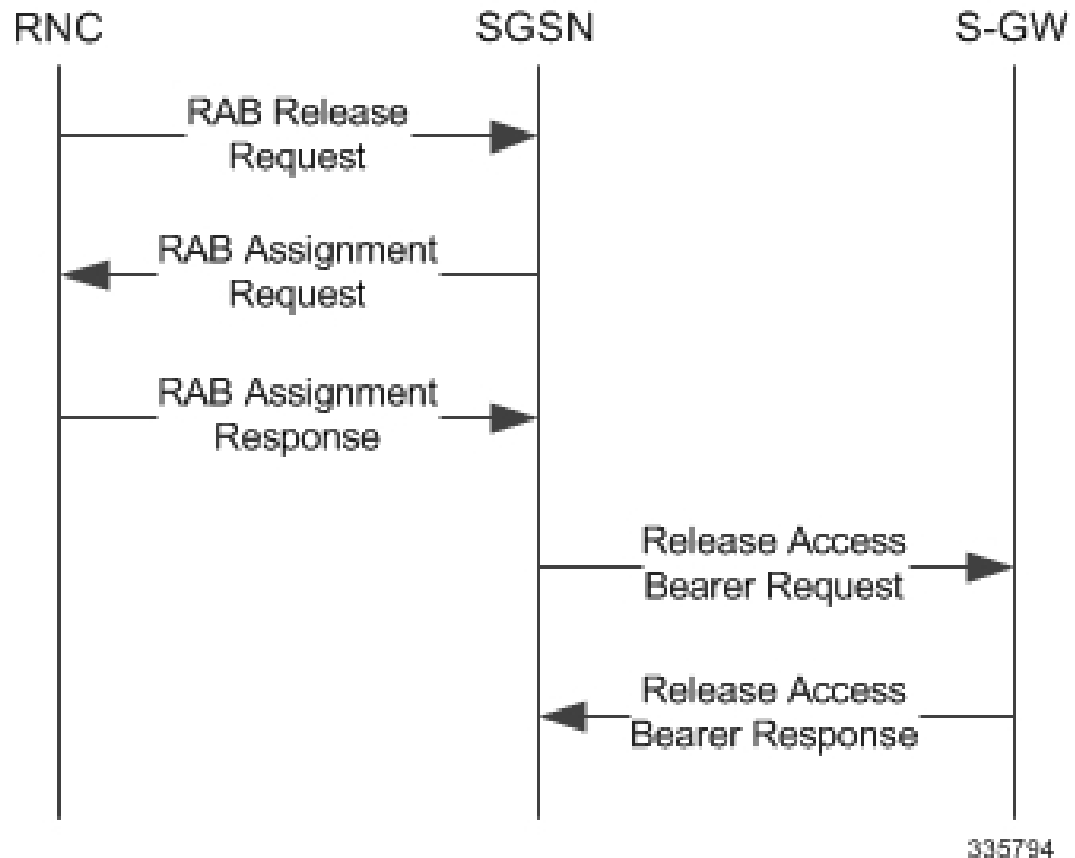
RAB Release with Direct Tunnel

If the SGSN receives a RAB Release Request from the RNC for bearer contexts activated with Direct Tunnel, it sends a Release Access Bearer Request to the S-GW.

Upon receiving the Release Access Bearer Request, the S-GW removes the S12 U RNC FTEID. If any downlink data appears, the S-GW sends a Downlink Data Notification because it does not have a user plane FTEID with which to forward data.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming/conversational bearers upon RAB release.

Figure 40: RAB Release Procedure with Direct Tunnel



Important

Operators should not use conversational or streaming class bearers in S4-SGSN.

Iu Release with Direct Tunnel

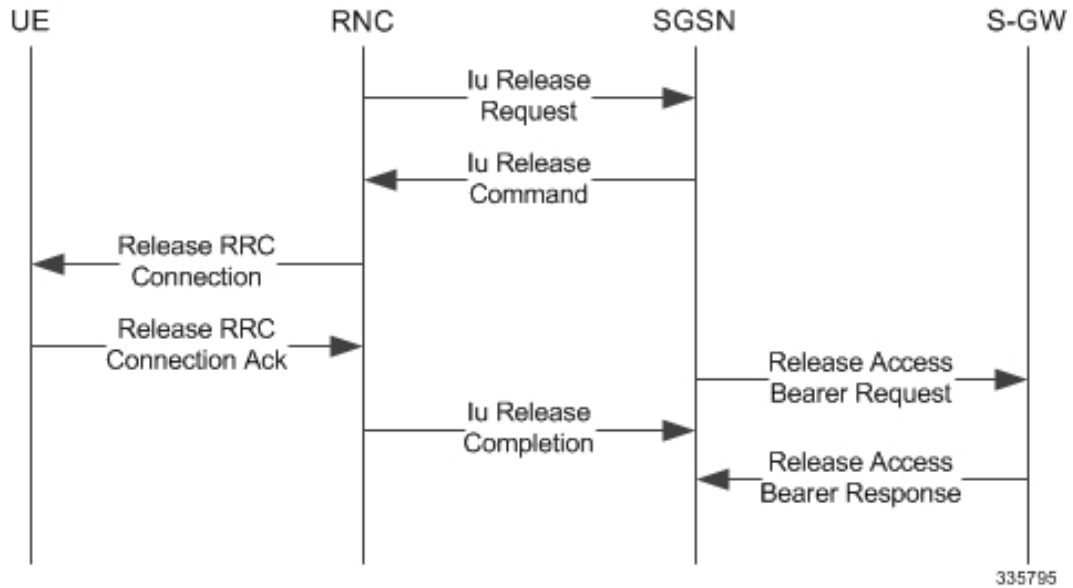
If the SGSN receives an Iu Release and bearers are activated with direct tunneling, it sends a Release Access Bearer Request to the S-GW.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming or conversational bearers upon Iu release.

**Important**

Operators should not use conversational or streaming class bearers in S4-SGSN.

Figure 41: Iu Release Procedure with Direct Tunnel

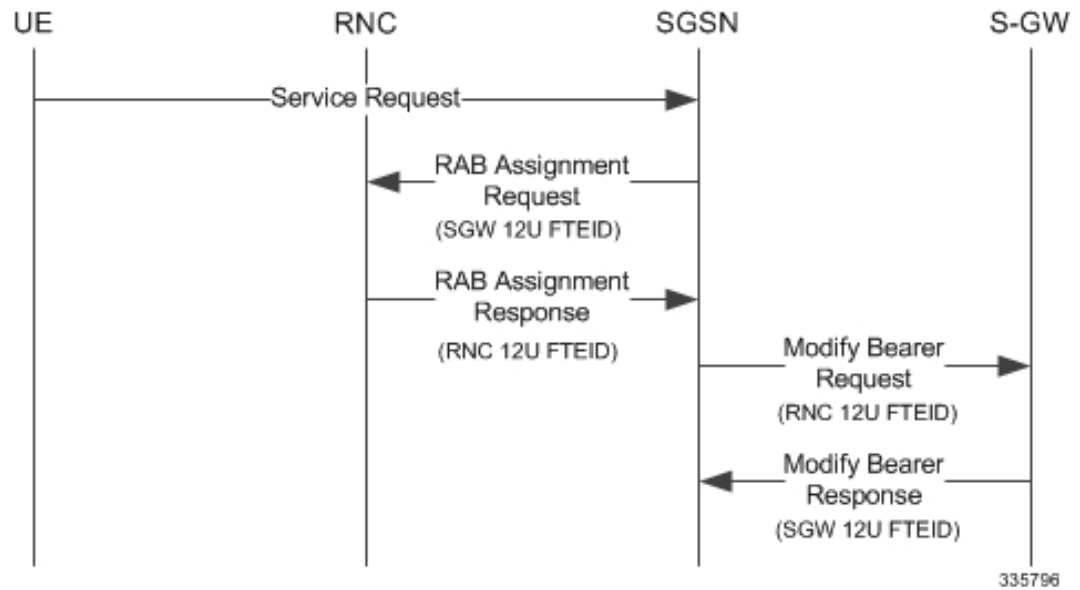


Service Request with Direct Tunnel

When a UE is Idle and wants to establish a data or signaling connection, it sends a Service Request for data. Alternatively a UE can also send a Service Request to the SGSN when it is paged by the SGSN.

Upon receiving a Service Request for data, the SGSN establishes RABs and sends a Modify Bearer Request to the S-GW with the 12U FTEID received from the RNC.

Figure 42: Service Request Procedure with Direct Tunnel



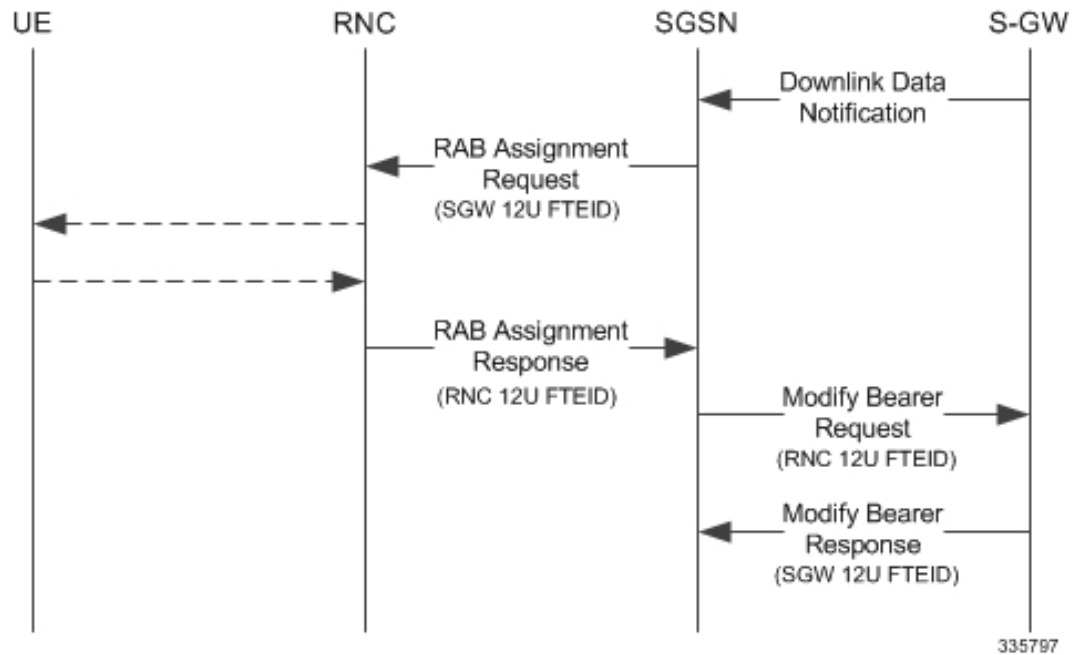
Downlink Data Notification with Direct Tunnel when UE in Connected State

When RABs are released (but UE retains an Iu connection with the SGSN), the SGSN notifies the S-GW to release the RNC side TEIDs via a Release Access Bearer Request.

If the S-GW receives any downlink GTPU data from the P-GW after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification message from the S-GW.

If the Downlink Data Notification is received from the S-GW, all of the missing RABs are established and a Modify Bearer Request is sent to the S-GW with the RNC S12U FTEID

Figure 43: Downlink Data Notification with Direct Tunnel



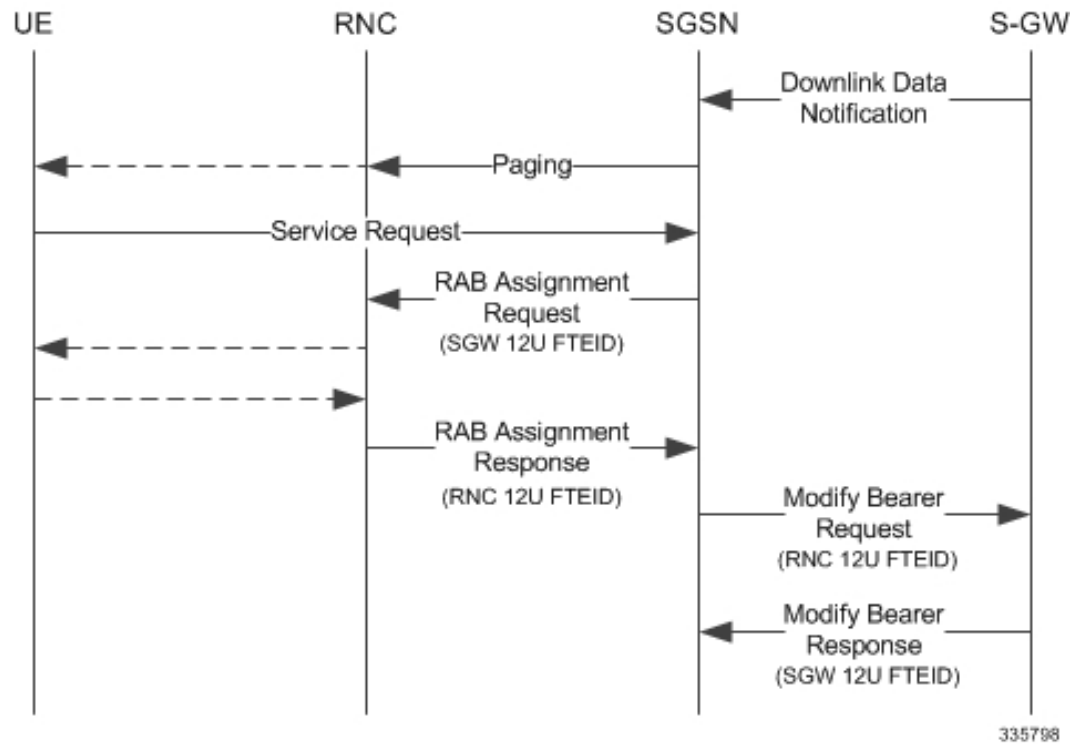
Downlink Data Notification with Direct Tunnel when UE in Idle State

When an Iu is released the UE goes IDLE. The SGSN informs the S-GW to release the RNC side TEIDs by sending a Release Access Bearer Request. After this point if the S-GW receives any downlink GTPU data from the P-GW, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data.

If the S-GW receives any downlink GTPU data after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification from the S-GW. If a Downlink

Data Notification is received from S-GW when the UE is idle, the SGSN pages the UE before establishing the RABs. The SGSN sends a Modify Bearer Request to the S-GW with the RNC S12U FTEID.

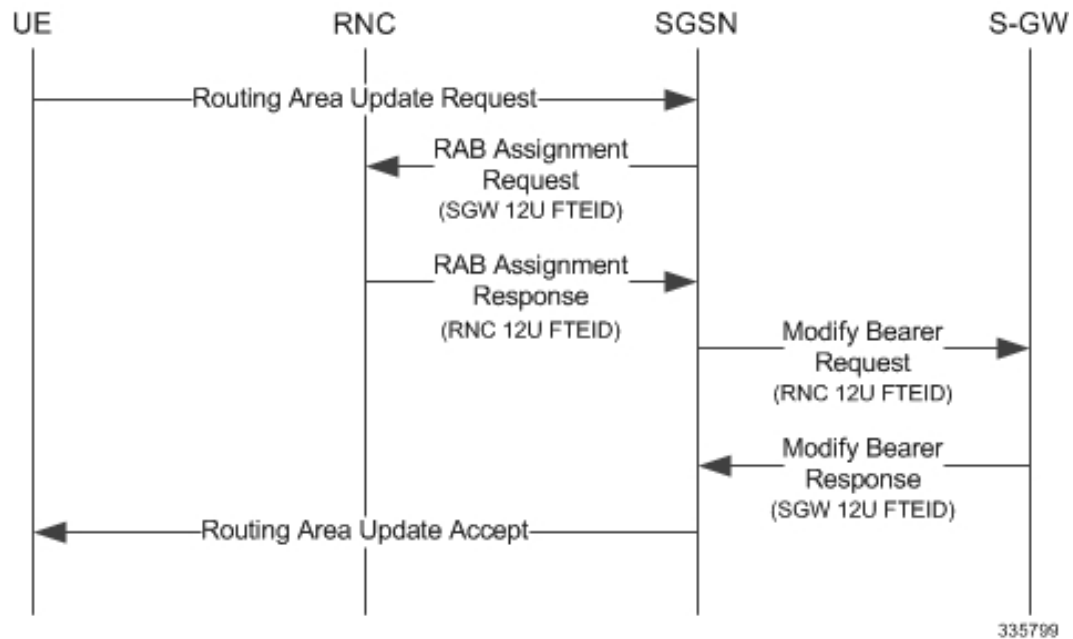
Figure 44: Downlink Data Notification when UE in Idle State



Intra SGSN Routing Area Update without SGW Change

For a Routing Area Update without an S-GW change with Direct Tunnel, the SGSN sends a Modify Bearer Request to the S-GW with the RNC FTEID. The SGSN will establish RABs with the target RNC only if the RABs were present with the source RNC.

Figure 45: Routing Area Update Procedure without SGW Change



The table below includes detailed behaviors for a Routing Area Update without S-GW change.

Table 16: Routing Area Update without S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs that are be modified and the rest released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.
Intra RAU	Not Present	No RAB	Supported	Yes	Supported	No	No RAB establishment with new RNC. MBR is sent with only PLMN change. Bearer Context will not carry any TEID.
Intra RAU	Present	No RAB	Supported	Yes	Supported	No	Same as above.
Intra RAU	Not Present	No RAB	Not Supported	No	Supported	No	No RAB establishment with new RNC. Modify Bearer Request to S-GW with DTF set and no user FTEID.
Intra RAU	Present	No RAB	Not Supported	No	Supported	No	Same as above.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Not Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs to be modified and the rest to be released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID. Modify Bearer.
Intra RAU	Not Present	No RAB	Not Supported	Yes	Supported	No	No RAB establishment with new RNC. MBR is sent with only PLMN change. SGSN will page / Service req / establish RABs when a downlink data notification is received.
Intra RAU	Present	No RAB	Not Supported	Yes	Supported	No	Same as above.
Intra RAU: New RNC does not support Direct Tunnel. No SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	No	No RAB establishment with new RNC. SGSN sends Modify Bearer Request to S-GW with S4U TEID. If there is change in PLMN ID, then new PLMN ID will be carried.
Intra RAU	Present	No RAB	Supported	Do not care	No Supported	No	Same as above.

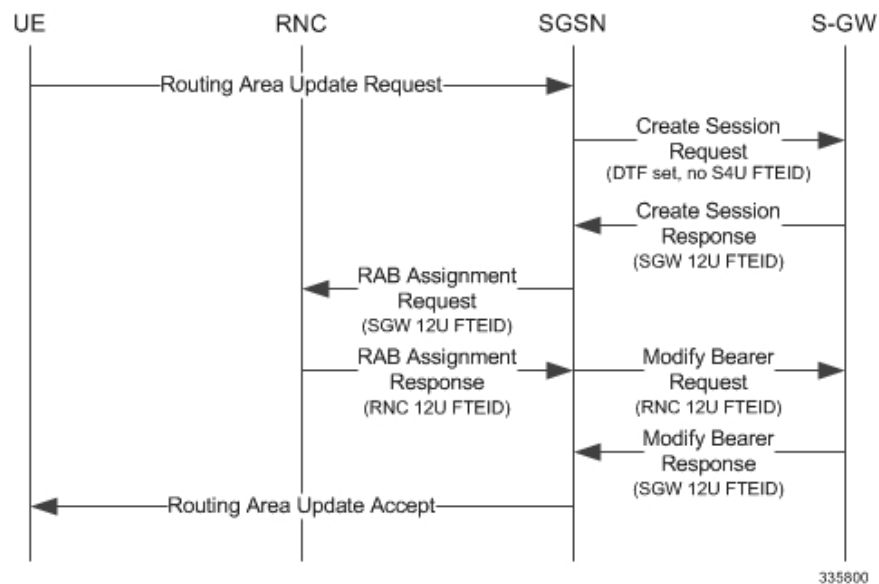
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Supported	Do not care	Not supported	No	Only the present RABs are established. MBR sent to S-GW with all bearers having S4U TEID. If there is change in PLMN ID, the new PLMN ID will be carried.

Routing Area Update with S-GW Change

In a Routing Area Update with an S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. In its Create Session Response, the S-GW sends an S12U FTEID which is forwarded to the RNC via a RAB Assignment Request.

The SGSN sends the RNC FTEID received in the RAB Assignment Response to the S-GW in a Modify Bearer Request. There are many scenarios to consider during Intra SGSN RAU.

Figure 46: Routing Area Update Procedure with SGW Change



The table below includes detailed behaviors for a Routing Area Update with S-GW change.

Table 17: Routing Area Update with S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU: Both RNCs support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U/S12U FTEID. S-GW will send its S12U TEID that SGSN stores as part of DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN will get DDN and establish RABs and send MBR.
Intra RAU	Present	No RAB	Supported	Do not care	Supported	Yes	Same as above.
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U/S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC. MBR will be initiated only with those RABs that are present rest of bearers to be removed.
Intra RAU: Old RNC does not support Direct Tunnel. SGW relocation							

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID that SGSN stores as part of our DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN gets DDN and establishes RABs and sends MBR.
Intra RAU	present	No RAB	Not Supported	Do not care	Supported	Yes	Same as above.
Intra RAU	Present	Some RABs	Not Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC and MBR will be initiated only with those RABs that are present and the rest as bearers to be removed.
Intra RAU: New RNC does not support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.

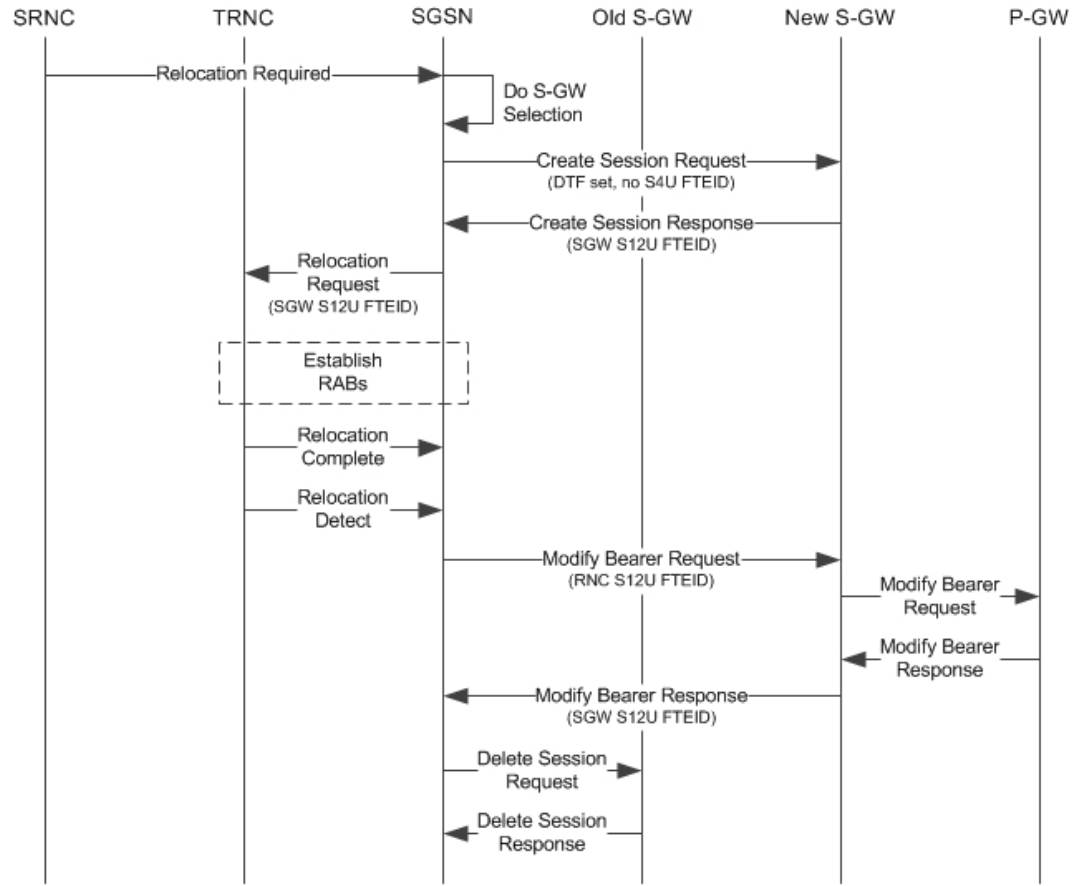
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	Some rABs	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID. No deactivation of PDPs.

Intra SRNS with S-GW Change

In Intra SRNS (Serving Radio Network Subsystem) with S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. The Create Session Response from the new S-GW contains the SGW S12U FTEID which the SGSN forwards to the Target RNC in a Relocation Request.

The SGSN sends the RNC S12U FTEID to the new S-GW in a Modify Bearer Request.

Figure 47: Intra SRNS with S-GW Change



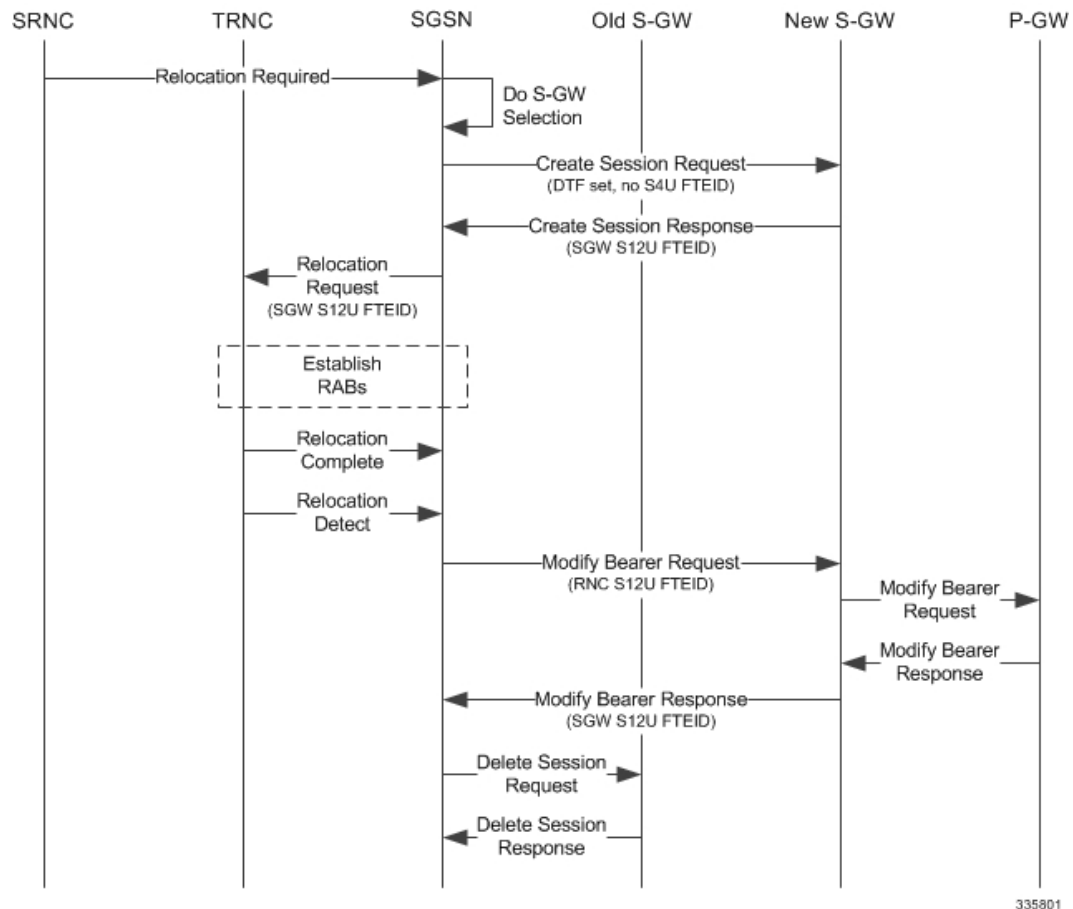
335801

The table below includes detailed behaviors for intra SRNS scenarios.

Intra SRNS without S-GW Change

In Intra SRNS without S-GW change, a Relocation Request is sent with SGW S12U FTEID. The RNC S12U FTEID received is forwarded to the S-GW in a Modify Bearer Request.

Figure 48: Intra SRNS without S-GW Change



335801

The table below includes detailed behaviors for intra SRNS scenarios.

Table 18: Intra SRNS Behaviors

Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12 U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Supported	Not Supported	No	Relocation Request to Target RNC is sent with SGSN S4 U FTEID. Modify Bearer Request to S-GW is sent with SGSN S4 U FTEID

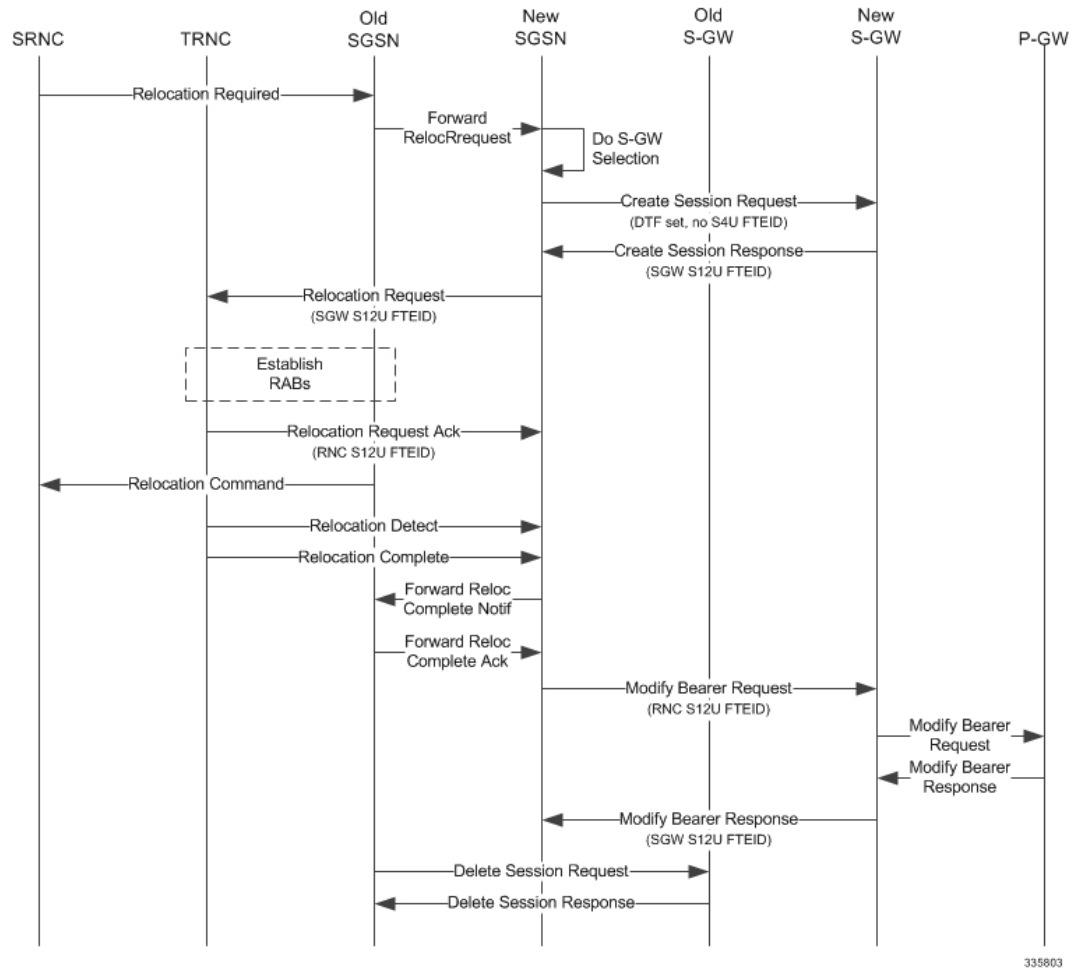
Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Not Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Not Supported	Supported	Yes	Create Session Request to new S-GW is sent with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response SGSN internally treats that as an S12U FTEID and continues the relocation. Relocation Request to Target RNC is sent with S12 U FTEID received in Create Session Response. Modify Bearer Request to new S-GW is sent with RNC S12U FTEID
Supported	Not Supported	Yes	Create Session Request to new SGW is sent with S4 U FTEID. Relocation Request to Target RNC is sent with SGSN U FTEID. Modify Bearer Request is sent with SGSN S4U FTEID.
Supported	Supported	Yes	SGSN sends a Create Session Request to new SGW with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response, SGSN will internally treat that as S12U FTEID and continue the relocation. Relocation Request to the Target RNC is sent with the S12 U FTEID received in the Create Session Response. Modify Bearer Request to new S-GW is sent with RNC U FTEID.

New SRNS with S-GW Change and Direct Data Transfer

The new SGSN sends a Create Session Request with DTF flag set and no user plane FTEID to the new S-GW.
The new SGSN sends the SGW S12U FTEID received in the Create Session Response in Relocation Request

to the Target RNC. The new SGSN sends the RNC S12U FTEID received in a Relocation Request Ack to the new S-GW in a Modify Bearer Request.

Figure 49: New SRNS with S-GW Change with Data Transfer

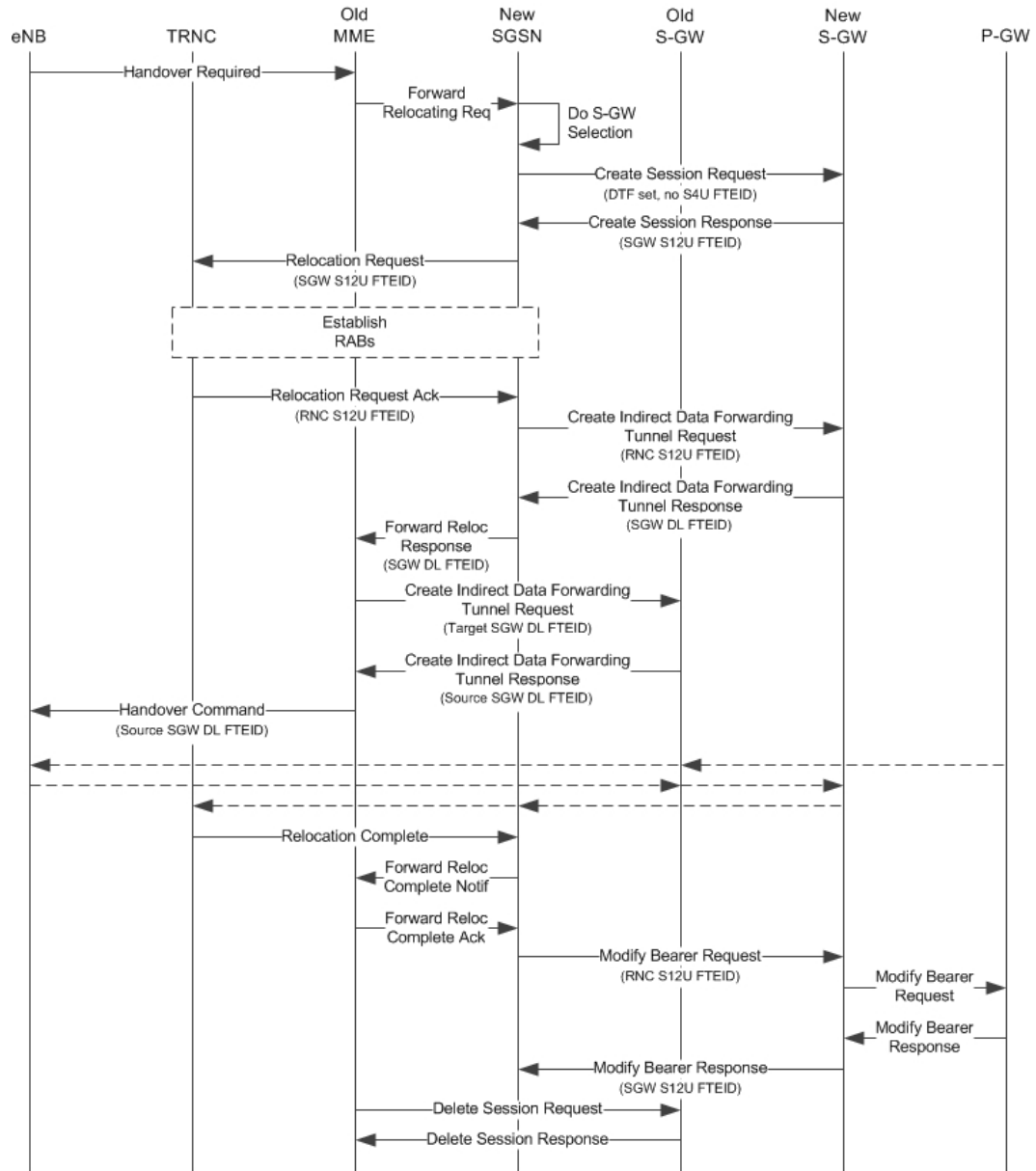


The table below includes detailed behaviors for New SRNS scenarios.

New SRNS with S-GW Change and Indirect Data Transfer

Indirect Data Transfer (IDFT) during a new SGSN SRNS happens during E-UTRAN-to-UTRAN connected mode IRAT handover. See the figure below for a detailed call flow.

Figure 50: New SRNS with S-GW Change and Indirect Data Transfer



335804

The table below includes detailed behaviors for New SRNS scenarios.

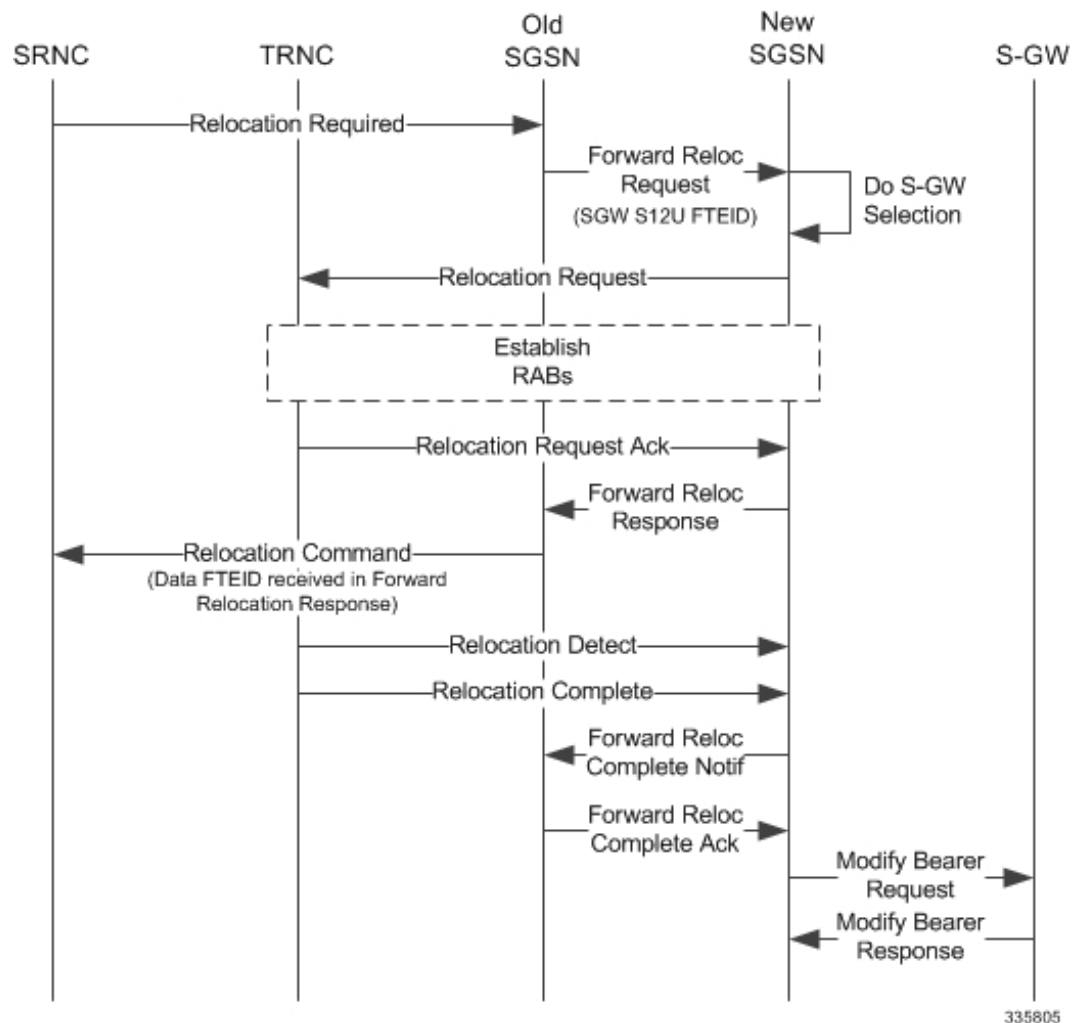
Table 19: New SRNS Behaviors

Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. SGSN includes RNC U FTEID in Forward Relocation Response. RNC U FTEID is also sent in Modify Bearer Request with DTF flag set.
Supported	Yes	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. In Forward Relocation Response RNC U FTEID is included. And in Modify Bearer Request RNC U FTEID is sent and DTF flag is set.
Supported	No	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. Create Indirect Data Forwarding Tunnel Request is sent with RNC FTEID received in Relocation Request Acknowledge. In Forward Relocation Response SGW DL U FTEID received in Create IDFT response is sent. Modify Bearer Request is sent with DTF set and RNC U FTEID.
Supported	Yes	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. In Forward Relocation Response RNC FTEID is sent and Modify Bearer Request is sent with DTF flag set and RNC U FTEID

Old SRNS with Direct Data Transfer

This scenario includes SRNS relocation between two SGSNs and hence IDFT is not applicable. Data will be forwarded between the source and target RNCs directly. Forward Relocation Request is sent with S12U FTEID.

Figure 51: Old SRNS with Direct Data Transfer



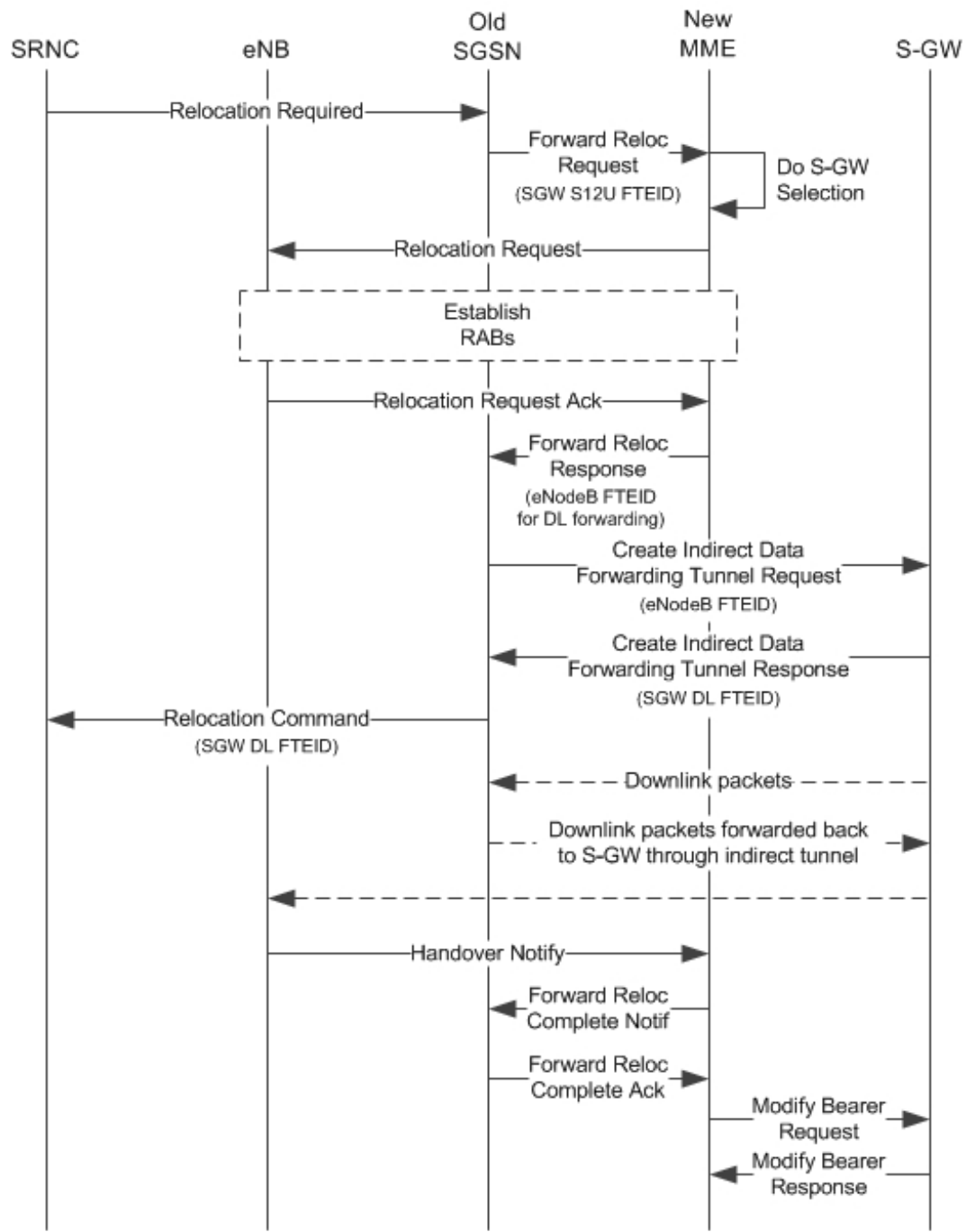
335805

The table below includes detailed behaviors for Old SRNS.

Old SRNS with Indirect Data Transfer

Indirect Data Transfer (IDFT) during Old SGSN SRNS happens during UTRAN-to-E-UTRAN connected mode IRAT handover. A Forward Relocation Request is sent with SGW S12U FTEID.

Figure 52: Old SRNS with Indirect Data Transfer 4



335806

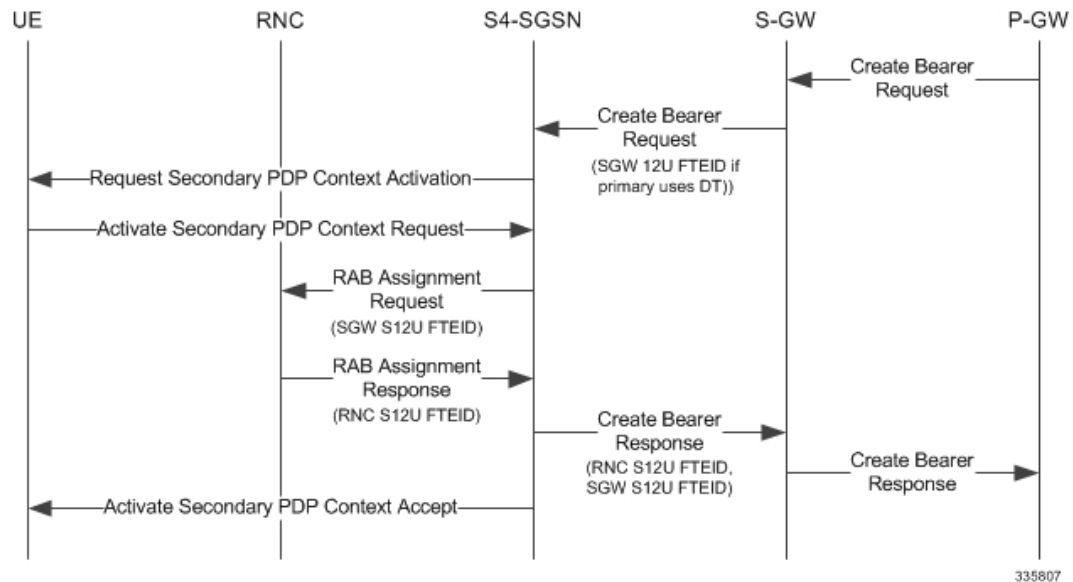
Table 20: Old SRNS Behaviors

Source RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Forward Relocation Request is send with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then a Create Indirect Data Forwarding Tunnel Request is sent with User plane FTEID received in the Forward Relocation Response. This will be the eNB user plane FTEID. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.
Supported	Yes	No	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC user plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.
Supported	No	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then Create Indirect Data Forwarding Tunnel Request is sent with eNB User plane FTEID received in the Forward Relocation Response. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.
Supported	Yes	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC use plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.

Network Initiated Secondary PDP Context Activation

The S-GW sends a Create Bearer Request for Network Initiated Secondary PDP Context Activation with the SGW S12U FTEID. This FTEID is sent in a RAB Assignment Request to the RNC. The RNC S12U FTEID received in the RAB Assignment Response is sent to the S-GW in a Create Bearer Response.

Figure 53: Network Initiated Secondary PDP Context Activation 5

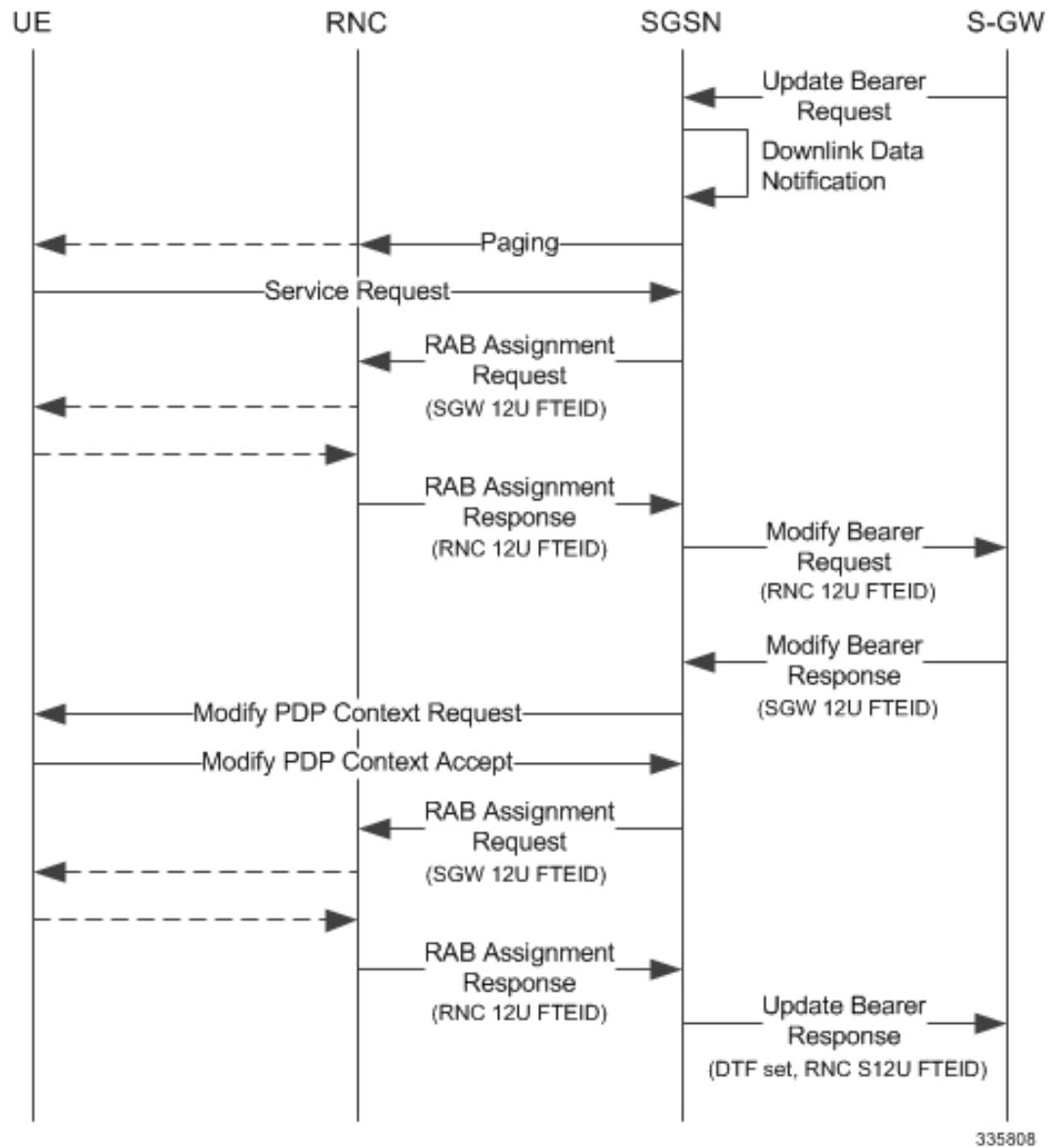


PGW Init Modification when UE is Idle

If UE is in IDLE state and PGW Init Modification is received, the SGSN sends the first MBR. Upon getting PGW Init Modification in Idle State, the SGSN queues the PGW Init Modification and feeds a Downlink Data

Notification internally. This sets up all RABs (using old QoS) and sends a Modify Bearer Request. When the Downlink Data Procedure is completed, the queued PGW Init Modification is processed.

Figure 54: PGW Init Modification when UE in Idle State



Limitations

During an intra RAU, intra SRNS or Service Request triggered by RAB establishment, if a few RABs fail the Modify Bearer Request the SGSN will mark those RABs as bearers to be removed. Under current specifications, it is not possible to send a Modify Bearer Request with a few bearers having S12U U-FTEIDs and a few bearers not having U-FTEIDs.

There is an ongoing CR at 3GPP to allow such Modify Bearer Requests and the S-GW should send DDN when it gets downlink data for the bearers that did not have U-FTEIDs. If this CR is approved, the SGSN will support (in a future release) sending a partial set of bearers with S12U FTEID and some bearers without any U-FTEID.

Standards Compliance

The Direct Tunnel complies with the following standards:

- 3GPP TS 23.060 version 10 sec 9.2.2 General Packet Radio Service (GPRS) Service description
- 3GPP TS 29.274 v10.5.0 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C)

Configuring Support for Direct Tunnel

The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN and S-GW are the only products that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

By default, direct tunnel support is

- *disallowed* on the SGSN/S-GW
- *allowed* on the GGSN/P-GW

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the operator policy named *default*. If direct tunnel is allowed in the *default* operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*. For more information about the purpose and uses of operator policies, refer to the section *Operator Policy*.

Configuring Direct Tunnel on an S4-SGSN

Configuration of a GTP-U direct tunnel (DT) requires enabling DT both in a call control profile and for the RNC.



Important

Direct tunneling must be enabled at both end points to allow direct tunneling for the MS/UE.

Enabling Setup of GTP-U Direct Tunnel

The SGSN determines whether a direct tunnel can be setup and by default the SGSN does not support direct tunnel. The following configuration enables a GTP-U DT in a call control profile:

```
config
  call-control-profile policy_name
```

```
direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Beginning with Release 19.3.5, **to-ggsn** and **to-sgw** options have been added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
 - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
 - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
 - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel to RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service. Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC. By default, DT functionality is enabled for all RNCs.

The following configuration sequence enables DT to a specific RNC that had been previously disabled for direct tunneling:

```
config
context ctxt_name
  iups-service service_name
    rnc id rnc_id
      default direct-tunnel
    end
```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference*.

Restricting Direct Tunnels

The following configuration scenario prohibits the S4-SGSN to setup direct tunneling over the S12 interface during Inter SGSN RAUs:

```
config
  call-control-profile profile_name
    rau-inter avoid-s12-direct-tunnel
  end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
  context context_name
    iups-service service_name
      rnc id rnc_id
        direct-tunnel not-permitted-by-rnc
      end
    end
```

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

show call-control-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
.
.
.
Re-Authentication
      : Disabled
Direct Tunnel
      : Not Restricted
GTPU Fast Path
      : Disabled
.
.
```

Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

show iups-service name *<service_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name                               : iups1
.
.
.
Available RNC:
  Rnc-Id                                     : 1
  Direct Tunnel                             : Not Restricted
```

Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the S4 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the S-GW over the S11 interfaces. The S-GW responds with its own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

Use the following example to configure this feature:

```
configure
context egress_context_name -noconfirm
  interface s12_interface_name
    ip address s12_ipv4_address_primary
    ip address s12_ipv4_address_secondary
  exit
port ethernet slot_number/port_number
  no shutdown
  bind interface s12_interface_name egress_context_name
exit
context egress_context_name -noconfirm
  gtpu-service s12_gtpu_egress_service_name
    bind ipv4-address s12_interface_ip_address
  exit
  egtp-service s12_egtp_egress_service_name
    interface-type interface-sgw-egress
    validation-mode default
    associate gtpu-service s12_gtpu_egress_service_name
    gtpc bind address s12_interface_ip_address
  exit
  sgw-service sgw_service_name -noconfirm
    associate egress-proto gtp egress-context egress_context_name egtp-service
s12_egtp_egress_service_name
end
```

Notes:

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

Monitoring and Troubleshooting Direct Tunnel

show subscribers sgsn-only

The output of this command indicates whether Direct Tunnel has been established.

show subscribers sgsn-only full all

```
Username: 123456789012345
Access Type: sgsn-pdp-type-ipv4      Network Type: IP
Access Tech: WCDMA UTRAN
|
```

```

|
NSAPI: 05                               Context Type: Primary
Context initiated by: MS
Direct Tunnel : Established

```

show gmm-sm statistics sm-only

The output of this command indicates the number of total active PDP contexts with direct tunnels.

show gmm-sm statistics sm-only

```

Activate PDP Contexts:
Total Actv PDP Ctx:
  3G-Actv Pdp Ctx:      1  2G-Avtv Pdp Ctx:      0
  Gn Interface:        1  Gn Interface:      0
  S4 Interface:        1  S4 Interface:      0
Total Actv Pdp Ctx:
with Direct Tunnel:    1

```

Direct Tunnel Bulk Statistics

Currently there are no bulk statistics available to monitor the number of PDP contexts with Direct Tunnel.

Bulk statistics under the EGTPC schema are applicable for both Direct Tunnel and Idle Mode Signalling Reduction (ISR) [3G and 2G]. The following statistics track the release access bearer request and response messages which are sent by the SGSN to the S-GW upon Iu or RAB release when either a direct tunnel or ISR is active:

- tun-sent-relaccbearreq
- tun-sent-retransrelaccbearreq
- tun-recv-relaccbearresp
- tun-recv-relaccbearrespDiscard
- tun-recv-relaccbearrespaccept
- tun-recv-relaccbearrespdenied

The following bulkstats under EGTPC schema track Downlink Data Notification (DDN) Ack and failure messages between the S-GW and the SGSN when either direct tunnel or ISR is active:

- tun-recv-dlinknotif
- tun-recv-dlinknotifDiscard
- tun-recv-dlinknotifNorsp
- tun-recv-retransdlinknotif
- tun-sent-dlinknotifackaccept
- tun-sent-dlinknotifackdenied
- tun-sent-dlinkdatafail

For complete descriptions of these variables, see the EGTPC Schema Statistics chapter in the *Statistics and Counters Reference*.



Embed IMSI into Session Id

- [Feature Summary and Revision History, page 285](#)
- [Feature Description, page 286](#)
- [How It Works, page 286](#)
- [Limitations, page 287](#)
- [Configuring Diameter Accounting Interim Interval, page 287](#)
- [Monitoring and Troubleshooting, page 288](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	<ul style="list-style-type: none">• GGSN• P-GW• SAEGW• S-GW
Applicable Platform(s)	<ul style="list-style-type: none">• ASR 5500• VPC - Di• VPC - Si
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable

Related Documentation	<ul style="list-style-type: none"> • <i>Command Line Interface Reference</i> • <i>GGSN Administration Guide</i> • <i>P-GW Administration Guide</i> • <i>SAEGW Administration Guide</i> • <i>S-GW Administration Guide</i>
-----------------------	--

Revision History

Revision Details	Release
First introduced.	21.3

Feature Description

For troubleshooting and investigating network issues related to the Diameter interface, it is important to filter the subscriber or UE specific Diameter traffic. Any traffic associated with a particular IMSI can be easily filtered, even without knowing the Diameter session ID, if the IMSI information is embedded into the Diameter Session ID AVP. This feature allows the operator to filter the subscriber or UE specific Diameter traffic.

This feature introduces a new CLI command **session-id include imsi** under the **diameter endpoint configuration** mode to embed IMSI into Diameter session ID AVP over the Gx, Gy, and Gz (Rf) interface.



Important

This feature is license controlled. Contact your Cisco account representative for information on how to obtain a license.

How It Works

A new CLI command **session-id include imsi** has been added under the **diameter endpoint configuration** mode to enable/disable inclusion of IMSI in Session-Id AVP for all Diameter sessions associated with that Diameter endpoint. Operators can enable only the required Diameter endpoints and control the inclusion of IMSI in the Session-ID AVP. IMSI information is included in the Diameter Session-ID AVP over the Gx, Gy, and Gz (Rf) interface, if the **session-id include imsi** is enabled on respective Diameter endpoints.

For emergency call with "only IMEI", IMSI information is not available for that emergency PDN. Hence, this IMSI information is not included in Diameter Session-ID at Gx, Gy, and Gz interface, when **session-id include imsi** is enabled. Configuring **session-id include imsi** impacts only new PDN connection and does not have any impact on existing PDN connection behavior (Gx, Gy, and Gz (Rf)) interface. For example, if the CLI command to include IMSI is enabled for the Gy Diameter endpoint after PDN creation. If a new dedicated bearer is created after this configuration change, then in this case Gy session established for a new dedicated bearer is not included IMSI in Gy Diameter session ID.

There is no impact of session manager recovery/ICSR on the session-ID AVP. Session-ID associated with Gx, Gy, and Gz (Rf) session is recovered transparently (which is irrespective of latest endpoint configuration). New sessions come up with session IDs as per the configuration on the newly active chassis.

Limitations

Following are the known limitations of this feature:

- Assuming IMSI information as sensitive information, operator must consider security aspects before enabling this CLI option.
- For an emergency call with "Only IMEI", IMSI information is not available for the emergency PDN, hence it is not included in the diameter Session-ID at Gx, Gy, and Gz (Rf) interface.
- During ICSR upgrade scenario, it is assumed that the new CLI option must be enabled only when the upgraded chassis is in stable state and there exists no chances of ICSR downgrade.
- If new CLI is enabled in the newer version of chassis, ICSR Downgrade is not recommended.
- As new CLI option is not available in old software versions, hence ICSR downgrade is not recommended. Performing ICSR downgrade should have the following impact on the diameter sessions, which have IMSI, included as part of Session-ID.
 - Gx and Gy: Existing diameter session (Gx, Gy) should be downgraded with old format of Session-Id. In that case, both P-GW and PCRF are out of sync leading to hanging session at P-GW or/and PCRF. Any communication from PCRF (RAR)/P-GW (CCR-U) can lead to stale session deletion.
 - Gz (Rf): However, Rf sessions should be recovered properly and any Rf signaling is sent out to Rf servers properly but responses cannot be processed as diamproxy cannot parse the new format session id which again puts Rf sessions into stale state until purged.

Configuring Diameter Accounting Interim Interval

The following CLI command has been added under the **diameter endpoint** configuration mode to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf). Configuration changes will be applicable only to new Sessions at Gx, Gy and Rf. Configuration changes will not have any impact on existing sessions behavior at Gx, Gy, and Rf. For Gy, multiple Diameter sessions can be initiated per subscriber and the session ID format setting will bind to the subscriber. The setting will be taken to effect when the first Diameter session is established and following Gy sub sessions will keep using the session ID format used in first session.

```
configure
  context context_name
    diameter endpoint endpoint_name
      [no] session-id include imsi
    end
```

Notes:

- **session-id:** Describes Diameter Session-ID format
- **include:** Includes configured information in Diameter Session-ID

- **imsi:** Includes International Mobile Subscriber Identification (IMSI) in Diameter Session-ID
- **no:** Disables this feature, that is, IMSI is not included in the Diameter Session-ID, which is the default behavior.
- By default, CLI is disabled, hence IMSI will not be populated in Diameter Session-ID.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the feature.

show configuration

The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi

show configuration [verbose]

The output of the above command is modified to display the following new field depending on whether the CLI is enabled or disabled:

- session-id include imsi
- no session-id include imsi



Extended QCI Options

This chapter describes extended QCI functionality.

- [Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters, page 289](#)
- [DSCP Marking Based on Both QCI and ARP Values, page 301](#)
- [New Standard QCI Support, page 304](#)
- [Non-standard QCI Support, page 338](#)

Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Feature Description

This section describes the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Support for QCI and ARP Visibility

As of StarOS release 20.2, the software has been enhanced to support the viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

ARP is a 3GPP mechanism for dropping or downgrading lower-priority bearers in situations where the network becomes congested. The network looks at the ARP when determining if new dedicated bearers can be established through the radio base station. QCI is an operator provisioned value that controls bearer level packet forwarding treatments.

This enhancement enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

**Important**

For the ARP value only the priority level value in the Allocation/Retention Priority (ARP) Information Element (IE) is considered. Pre-emption Vulnerability (PVI) and Pre-emption Capability (PCI) flags in the ARP IE are not considered.

The existing **show apn statistics name** *apn-name* and **show apn statistics Exec Mode** CLI commands have been enhanced. The output of these commands now provides visibility for QoS statistics on a QCI/ARP basis.

Licensing**Important**

ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring ARP Granularity for QCI Level Counters

This section describes how to configure the ARP Granularity for QCI Level Counters feature.

**Important**

ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

Configuring the feature consists of the following tasks:

- 1 Create a Stats Profile.
- 2 Enable the Collection of Per QCI Packet Drop Counters.
- 3 Enable the Collection of QCI/ARP Level Statistics.
- 4 Associate a Stats Profile with an APN.
- 5 Verify the Configuration.

Create a Stats Profile

Use the following example to access *Global Configuration Mode* and create a Stats Profile:

```
configure
stats-profile stats_profile_name
end
```

Notes:

- *stats_profile_name* must be an alphanumeric string from 1 to 63 characters in length.

Enable the Collection of Packet Drop Statistics

Use the following example to access *Stats Profile Configuration Mode* and create a Stats Profile and enable the collection of packet drop statistics:

```
configure
stats-profile stats_profile_name
packet-drop
end
```

To disable the collection of packet drop statistics

```
configure
stats-profile stats_profile_name
no packet-drop
end
```

Notes:

- *stats_profile_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- **packet-drop**: enables the collection of packet drop statistics for the specified Stats Profile.
- **no packet-drop**: disables the collection of packet drop statistics for the specified Stats Profile.

Enable the Collection of QCI/ARP Level Statistics

Use the following example to access *Stats Profile Configuration Mode* and enable the collection of QCI/ARP level statistics for a Stats Profile:

```
configure
stats-profile stats_profile_name
qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 ] + } }
end
```

To disable the collection of QCI/ARP statistics:

```
configure
stats-profile stats_profile_name
no qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 ] + } }
end
```

Notes:

- *stats_profile_name* must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 64 characters in length.
- **qci**: configures the collection of ARP priority level statistics for the specified QCI(s).
- **non-std**: configures the collection of ARP priority level statistics for non-standard QCIs.
- **non-gbr**: configures the collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.
- **gbr**: configures the collection of ARP priority level statistics for non-standard GBR QCIs.
- **arp**: configures the collection of ARP priority level statistics for the specified ARP values.
- **no**: disables the collection of ARP priority level statistics for the specified **qci** and **arp** settings.

Associate a Stats Profile with an APN

Use the following example to access *APN Configuration Mode* and associate a Stats Profile with an APN:

```
configure
  apn apn_name
    stats-profile stats_profile_name
  end
```

To disassociate a Stats Profile from a specified APN:

```
configure
  apn apn_name
    no stats-profile
  end
```

Notes:

- *stats_profile_name*: must be the name of an existing Stats Profile. The name must be an alphanumeric string from 1 to 63 characters in length.
- A maximum of 64 Stats Profiles can be configured per P-GW/SAEGW/GGSN service.
- **no stats-profile**: disassociates the Stats Profile from the APN.



Important

If a Stats Profile is associated with more than 12 APNs, the following memory and performance impact warning is provided:

```
[WARNING] Configuring QCI/ ARP level statistics for more then 12 APNs will have
memory and performance impact. Do you want to continue [Y/N]
```

Verify the Configuration

Use the following procedure to verify the configuration:

First, verify that the Stats Profile is associated with the correct APN. In *Exec Mode*, enter the following command:

```
show apn name apn_name
```

Notes:

- In the command output, look for the **stats profile** field. It should contain the name of the Stats Profile which is associated with this APN.

Next, verify that the Stats Profile configuration settings are correct. In *Exec Mode*, enter the following command:

```
show stats-profile name stats_profile_name
```

Notes:

- Where *stats_profile_name* is the name of the Stats Profile for which you want to view settings.
- The command output includes the following information:
 - Stats Profile name
 - Packet-drop configuration settings for both QCI and ARP
 - QCI ARP combinations for which the StarOS will collect granular ARP statistics

If any of the above settings are incorrect, perform the configuration procedure again to reconfigure the Stats Profile with the proper settings.

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

This section describes how to monitor the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Bulk Statistics

This section provides the bulk statistics that have been added to support the ARP Granularity and per QCI Packet Drop Counters feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
```

```

qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70

```

Show Commands

This section provides the Exec Mode show commands that are available to support the Per Packet QCI Drop Counters and ARP Granularity for QCI Level Counters feature.

show apn statistics

The **qci** and **arp** keywords have been added to this command. The new keywords enable operators to view output for four basic scenarios that apply to the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.

Scenario 1

View packet drop counters with granularity at the QCI/ARP level for a single APN. The output of this command is useful for isolating network issues that may be affecting packet drops.

show apn statistics name *apn_name* **qci** { **all** | **1-9** | **non-std** { **gbr** | **non-gbr** } } **arp** { **all** | **1-15** }

Notes:

- **apn_name**: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 2

View packet drop counters with granularity at the QCI/ARP level for all APNs.

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } } arp { all | 1-15 }

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 3

View the new packet drop counters at granularity of QCI level, and pre-existing QCI level counters for the specified APN.

show apn statistics name apn_name qci { all | 1-9 | non-std { gbr | non-gbr } }

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.
- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

Scenario 4

View the packet drop counters at the granularity of the QCI level, and view pre-existing QCI counters consolidated for all APNs.

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } }

Notes:

- *apn_name*: must be the name of a configured APN created in *APN Configuration Mode*.

- **qci**: displays packet drop statistics for the specified QCI(s).
- **all**: displays packet drop statistics for all QCI(s).
- **1-9**: displays packet drop statistics for QCI <n>. Must be a QCI number from 1 to 9.
- **non-std**: displays packet drop statistics for non-standard QCIs.
- **non-gbr**: displays packet drop statistics for non-standard non-gbr QCIs
- **gbr**: displays packet drop statistics for non-standard GBR QCIs.
- **arp**: displays statistics for the specified ARP priority level(s)
- **all**: displays packet drop statistics for all ARP priority levels.
- **1-15**: displays statistics for the specified ARP priority level.

The output of the **show apn statistics name apn_name qci all arp all** command has been enhanced to display the following new statistics:

Data Statistics:

Uplink Bytes:	0	Downlink Bytes:	0
Uplink Pkts:	0	Downlink Pkts:	0
Uplink Bytes dropped:	0	Downlink Bytes dropped:	0
Uplink Pkts dropped:	0	Downlink Pkts dropped:	0

Uplink Dropped:	Downlink Dropped:	
MBR Exceeded(Bytes):	0	MBR Exceeded(Bytes):
MBR Exceeded(Pkts):	0	MBR Exceeded(Pkts):
AMBR Exceeded(Bytes):	0	AMBR Exceeded(Bytes):
AMBR Exceeded(Pkts):	0	AMBR Exceeded(Pkts):
Miscellaneous(Bytes):	0	Miscellaneous(Bytes):
Miscellaneous(Pkts):	0	Miscellaneous(Pkts):
Overcharge Prtctn(Bytes):	0	Overcharge Prtctn(Bytes):
Overcharge Prtctn(Pkts):	0	Overcharge Prtctn(Pkts):
SGW Restoration(Bytes):	0	SGW Restoration(Bytes):
SGW Restoration(Pkts):	0	SGW Restoration(Pkts):
SDF Gate(Bytes):	0	SDF Gate(Bytes):
SDF Gate(Pkts):	0	SDF Gate(Pkts):
ITC Gate(Bytes):	0	ITC Gate(Bytes):
ITC Gate(Pkts):	0	ITC Gate(Pkts):
Flow Terminated(Bytes):	0	Flow Terminated(Bytes):
Flow Terminated(Pkts):	0	Flow Terminated(Pkts):
Subsession Terminated(Bytes):	0	Subsession Terminated(Bytes):
Subsession Terminated(Pkts):	0	Subsession Terminated(Pkts):
Call Terminated(Bytes):	0	Call Terminated(Bytes):
Call Terminated(Pkts):	0	Call Terminated(Pkts):
DCCA Discard(Bytes):	0	DCCA Discard(Bytes):
DCCA Discard(Pkts):	0	DCCA Discard(Pkts):
No Rule Match(Bytes):	0	No Rule Match(Bytes):
No Rule Match(Pkts):	0	No Rule Match(Pkts):
ICAP(Bytes):	0	ICAP(Bytes):
ICAP(Pkts):	0	ICAP(Pkts):
SFW(Bytes):	0	SFW(Bytes):
SFW(Pkts):	0	SFW(Pkts):
Hierarchical ENF(Bytes):	0	Hierarchical ENF(Bytes):
Hierarchical ENF(Pkts):	0	Hierarchical ENF(Pkts):
Dynamic CA Gate(Bytes):	0	Dynamic CA Gate(Bytes):
Dynamic CA Gate(Pkts):	0	Dynamic CA Gate(Pkts):
NAT64 Cancel(Bytes):	0	NAT64 Cancel(Bytes):
NAT64 Cancel(Pkts):	0	NAT64 Cancel(Pkts):
Bearer Not Found(Bytes):	0	Bearer Not Found(Bytes):
Bearer Not Found(Pkts):	0	Bearer Not Found(Pkts):

4G Bearers Released By Reasons:

QCI1 QCI2 QCI3 QCI4 QCI5 QCI6 QCI7 QCI8 QCI9

Admin disconnect: 0 0 0 0 0 0 0 0

ARP level distribution of 4G Bearer Released By Reasons:

Admin disconnect:

QCI 1:

ARP 1:	0
ARP 2:	0
ARP 3:	0
ARP 4:	0
ARP 5:	0
ARP 6:	0
ARP 7:	0
ARP 8:	0
ARP 9:	0
ARP 10:	0
ARP 11:	0
ARP 12:	0
ARP 13:	0
ARP 14:	0
ARP 15:	0

.
.
.

QCI 9:

ARP 1:	0
ARP 2:	0
ARP 3:	0
ARP 4:	0
ARP 5:	0
ARP 6:	0
ARP 7:	0
ARP 8:	0
ARP 9:	0
ARP 10:	0
ARP 11:	0
ARP 12:	0
ARP 13:	0
ARP 14:	0
ARP 15:	0

Subscriber QoS Statistics:

4G Bearers Released By Reasons:

	QCI1	QCI2	QCI3	QCI4	QCI5	QCI6	QCI7	QCI8	QCI9
Admin disconnect:	0	0	0	0	0	0	0	0	0

ARP level distribution of 4G Bearer Released By Reasons:

Admin disconnect:

QCI 1:

ARP 1:	0
ARP 2:	0
ARP 3:	0
ARP 4:	0
ARP 5:	0
ARP 6:	0
ARP 7:	0
ARP 8:	0
ARP 9:	0
ARP 10:	0
ARP 11:	0
ARP 12:	0
ARP 13:	0
ARP 14:	0

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

```

        ARP 15:                0
        .
        .
        .

    QCI 9:
        ARP 1:                  0
        ARP 2:                  0
        ARP 3:                  0
        ARP 4:                  0
        ARP 5:                  0
        ARP 6:                  0
        ARP 7:                  0
        ARP 8:                  0
        ARP 9:                  0
        ARP 10:                 0
        ARP 11:                 0
        ARP 12:                 0
        ARP 13:                 0
        ARP 14:                 0
        ARP 15:                 0

    QCI 1:
    ARP 1:
        Bearer Active:          0   Bearer setup:                2
        Bearer Released:        2   Bearer Rejected:            0

        Uplink Bytes forwarded:  0   Downlink Bytes forwarded:  0
        Uplink Pkts forwarded:   0   Downlink Pkts forwarded:   0
        Uplink Bytes dropped:    0   Downlink Bytes dropped:    0
        Uplink Pkts dropped:     0   Downlink Pkts dropped:    0
    Uplink Dropped:
        MBR Exceeded(Bytes):     0   Downlink Dropped:
        MBR Exceeded(Pkts):      0   MBR Exceeded(Bytes):      0
        AMBR Exceeded(Bytes):    0   MBR Exceeded(Pkts):      0
        AMBR Exceeded(Pkts):     0   AMBR Exceeded(Bytes):    0
        Miscellaneous(Bytes):    0   AMBR Exceeded(Pkts):     0
        Miscellaneous(Pkts):     0   Miscellaneous(Bytes):    0
        Overcharge Prtctn(Bytes): 0   Miscellaneous(Pkts):     0
        Overcharge Prtctn(Pkts): 0   Overcharge Prtctn(Bytes): 0
        SGW Restoration(Bytes):  0   Overcharge Prtctn(Pkts): 0
        SGW Restoration(Pkts):   0   SGW Restoration(Bytes):  0
        SDF Gate(Bytes):         0   SGW Restoration(Pkts):   0
        SDF Gate(Pkts):         0   SDF Gate(Bytes):         0
        ITC Gate(Bytes):         0   SDF Gate(Pkts):         0
        ITC Gate(Pkts):         0   ITC Gate(Bytes):         0
        Flow Terminated(Bytes): 0   ITC Gate(Pkts):         0
        Flow Terminated(Pkts):  0   Flow Terminated(Bytes): 0
        Subsession Terminated(Bytes): 0   Flow Terminated(Pkts):  0
        Subsession Terminated(Pkts): 0   Subsession Terminated(Bytes): 0
        Call Terminated(Bytes):  0   Subsession Terminated(Pkts): 0
        Call Terminated(Pkts):   0   Call Terminated(Bytes):  0
        DCCA Discard(Bytes):      0   Call Terminated(Pkts):   0
        DCCA Discard(Pkts):      0   DCCA Discard(Bytes):      0
        No Rule Match(Bytes):     0   DCCA Discard(Pkts):      0
        No Rule Match(Pkts):     0   No Rule Match(Bytes):     0
        ICAP(Bytes):              0   No Rule Match(Pkts):     0
        ICAP(Pkts):               0   ICAP(Bytes):              N/A
        SFW(Bytes):               0   ICAP(Pkts):              N/A
        SFW(Pkts):                0   SFW(Bytes):               0
        Hierarchical ENF(Bytes):  0   SFW(Pkts):                0
        Hierarchical ENF(Pkts):   0   Hierarchical ENF(Bytes):  0
        Dynamic CA Gate(Bytes):   0   Hierarchical ENF(Pkts):   0
        Dynamic CA Gate(Pkts):    0   Dynamic CA Gate(Bytes):   : 0
        NAT64 Cancel(Bytes):      0   Dynamic CA Gate(Pkts):    0
        NAT64 Cancel(Pkts):       0   NAT64 Cancel(Bytes):      0
        Bearer Not Found(Bytes):  0   NAT64 Cancel(Pkts):       0
        Bearer Not Found(Pkts):   0   Bearer Not Found(Bytes):  0
    QCI 1:
    ARP 2:
        Bearer Active:          0   Bearer setup:                2
        Bearer Released:        2   Bearer Rejected:            0

```

Uplink Bytes forwarded:	0	Downlink Bytes forwarded:	0
Uplink Pkts forwarded:	0	Downlink Pkts forwarded:	0
Uplink Bytes dropped:	0	Downlink Bytes dropped:	0
Uplink Pkts dropped:	0	Downlink Pkts dropped:	0
Uplink Dropped:		Downlink Dropped:	
MBR Exceeded(Bytes):	0	MBR Exceeded(Bytes):	0
MBR Exceeded(Pkts):	0	MBR Exceeded(Pkts):	0
AMBR Exceeded(Bytes):	0	AMBR Exceeded(Bytes):	0
AMBR Exceeded(Pkts):	0	AMBR Exceeded(Pkts):	0
Miscellaneous(Bytes):	0	Miscellaneous(Bytes):	0
Miscellaneous(Pkts):	0	Miscellaneous(Pkts):	0
Overcharge Prtctn(Bytes)	0	Overcharge Prtctn(Bytes):	0
Overcharge Prtctn(Pkts):	0	Overcharge Prtctn(Pkts):	0
SGW Restoration(Bytes):	0	SGW Restoration(Bytes):	0
SGW Restoration(Pkts):	0	SGW Restoration(Pkts):	0
SDF Gate(Bytes):	0	SDF Gate(Bytes):	0
SDF Gate(Pkts):	0	SDF Gate(Pkts):	0
ITC Gate(Bytes):	0	ITC Gate(Bytes):	0
ITC Gate(Pkts):	0	ITC Gate(Pkts):	0
Flow Terminated(Bytes):	0	Flow Terminated(Bytes):	0
Flow Terminated(Pkts):	0	Flow Terminated(Pkts):	0
Subsession Terminated(Bytes):	0	Subsession Terminated(Bytes):	0
Subsession Terminated(Pkts):	0	Subsession Terminated(Pkts):	0
Call Terminated(Bytes):	0	Call Terminated(Bytes):	0
Call Terminated(Pkts):	0	Call Terminated(Pkts):	0
DCCA Discard(Bytes):	0	DCCA Discard(Bytes):	0
DCCA Discard(Pkts):	0	DCCA Discard(Pkts):	0
No Rule Match(Bytes):	0	No Rule Match(Bytes):	0
No Rule Match(Pkts):	0	No Rule Match(Pkts):	0
ICAP(Bytes):	0	ICAP(Bytes):	N/A
ICAP(Pkts):	0	ICAP(Pkts):	N/A
SFW(Bytes):	0	SFW(Bytes):	0
SFW(Pkts):	0	SFW(Pkts):	0
Hierarchical ENF(Bytes):	0	Hierarchical ENF(Bytes):	0
Hierarchical ENF(Pkts):	0	Hierarchical ENF(Pkts):	0
Dynamic CA Gate(Bytes):	0	Dynamic CA Gate(Bytes):	0
Dynamic CA Gate(Pkts):	0	Dynamic CA Gate(Pkts):	0
NAT64 Cancel(Bytes):	0	NAT64 Cancel(Bytes):	0
NAT64 Cancel(Pkts):	0	NAT64 Cancel(Pkts):	0
Bearer Not Found(Bytes):	0	Bearer Not Found(Bytes):	0
Bearer Not Found(Pkts):	0	Bearer Not Found(Pkts):	0

The output of the **show apn statistics name *apn_name* qci all** command has been enhanced to display the following new statistics:

Data Statistics:

Uplink Bytes:	0	Downlink Bytes:	0
Uplink Pkts:	0	Downlink Pkts:	0
Uplink Bytes dropped:	0	Downlink Bytes dropped:	0
Uplink Pkts dropped:	0	Downlink Pkts dropped:	0
Uplink Dropped:		Downlink Dropped:	
MBR Exceeded(Bytes):	0	MBR Exceeded(Bytes):	0
MBR Exceeded(Pkts):	0	MBR Exceeded(Pkts):	0
AMBR Exceeded(Bytes):	0	AMBR Exceeded(Bytes):	0
AMBR Exceeded(Pkts):	0	AMBR Exceeded(Pkts):	0
Miscellaneous(Bytes):	0	Miscellaneous(Bytes):	0
Miscellaneous(Pkts):	0	Miscellaneous(Pkts):	0
Overcharge Prtctn(Bytes)	0	Overcharge Prtctn(Bytes):	0
Overcharge Prtctn(Pkts):	0	Overcharge Prtctn(Pkts):	0
SGW Restoration(Bytes):	0	SGW Restoration(Bytes):	0
SGW Restoration(Pkts):	0	SGW Restoration(Pkts):	0
SDF Gate(Bytes):	0	SDF Gate(Bytes):	0
SDF Gate(Pkts):	0	SDF Gate(Pkts):	0
ITC Gate(Bytes):	0	ITC Gate(Bytes):	0
ITC Gate(Pkts):	0	ITC Gate(Pkts):	0
Flow Terminated(Bytes):	0	Flow Terminated(Bytes):	0
Flow Terminated(Pkts):	0	Flow Terminated(Pkts):	0
Subsession Terminated(Bytes):	0	Subsession Terminated(Bytes):	0
Subsession Terminated(Pkts):	0	Subsession Terminated(Pkts):	0
Call Terminated(Bytes):	0	Call Terminated(Bytes):	0
Call Terminated(Pkts):	0	Call Terminated(Pkts):	0

Monitoring Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters

DCCA Discard(Bytes):	0	DCCA Discard(Bytes):	0
DCCA Discard(Pkts):	0	DCCA Discard(Pkts):	0
No Rule Match(Bytes):	0	No Rule Match(Bytes):	0
No Rule Match(Pkts):	0	No Rule Match(Pkts):	0
ICAP(Bytes):	0	ICAP(Bytes):	N/A
ICAP(Pkts):	0	ICAP(Pkts):	N/A
SFW(Bytes):	0	SFW(Bytes):	0
SFW(Pkts):	0	SFW(Pkts):	0
Hierarchical ENF(Bytes):	0	Hierarchical ENF(Bytes):	0
Hierarchical ENF(Pkts):	0	Hierarchical ENF(Pkts):	0
Dynamic CA Gate(Bytes):	0	Dynamic CA Gate(Bytes):	:
Dynamic CA Gate(Pkts):	0	Dynamic CA Gate(Pkts):	0
NAT64 Cancel(Bytes):	0	NAT64 Cancel(Bytes):	0
NAT64 Cancel(Pkts):	0	NAT64 Cancel(Pkts):	0
Bearer Not Found(Bytes):	0	Bearer Not Found(Bytes):	0
Bearer Not Found(Pkts):	0	Bearer Not Found(Pkts):	0

4G Bearers Released By Reasons:

	QCI1	QCI2	QCI3	QCI4	QCI5	QCI6	QCI7	QCI8	QCI9
Admin disconnect:	0	0	0	0	0	0	0	0	0

Subscriber QoS Statistics:

QCI 1:			
Bearer Active:	0	Bearer setup:	0
Bearer Released:	0	Bearer Rejected:	0
Uplink Bytes forwarded:	0	Downlink Bytes forwarded:	0
Uplink Pkts forwarded:	0	Downlink Pkts forwarded:	0
Uplink Bytes dropped:	0	Downlink Bytes dropped:	0
Uplink Pkts dropped:	0	Downlink Pkts dropped:	0
Uplink Dropped:		Downlink Dropped:	
MBR Exceeded(Bytes):	0	MBR Exceeded(Bytes):	0
MBR Exceeded(Pkts):	0	MBR Exceeded(Pkts):	0
AMBR Exceeded(Bytes):	0	AMBR Exceeded(Bytes):	0
AMBR Exceeded(Pkts):	0	AMBR Exceeded(Pkts):	0
Miscellaneous(Bytes):	0	Miscellaneous(Bytes):	0
Miscellaneous(Pkts):	0	Miscellaneous(Pkts):	0
Overcharge Prtctn(Bytes):	0	Overcharge Prtctn(Bytes):	0
Overcharge Prtctn(Pkts):	0	Overcharge Prtctn(Pkts):	0
SGW Restoration(Bytes):	0	SGW Restoration(Bytes):	0
SGW Restoration(Pkts):	0	SGW Restoration(Pkts):	0
SDF Gate(Bytes):	0	SDF Gate(Bytes):	0
SDF Gate(Pkts):	0	SDF Gate(Pkts):	0
ITC Gate(Bytes):	0	ITC Gate(Bytes):	0
ITC Gate(Pkts):	0	ITC Gate(Pkts):	0
Flow Terminated(Bytes):	0	Flow Terminated(Bytes):	0
Flow Terminated(Pkts):	0	Flow Terminated(Pkts):	0
Subsession Terminated(Bytes):	0	Subsession Terminated(Bytes):	0
Subsession Terminated(Pkts):	0	Subsession Terminated(Pkts):	0
Call Terminated(Bytes):	0	Call Terminated(Bytes):	0
Call Terminated(Pkts):	0	Call Terminated(Pkts):	0
DCCA Discard(Bytes):	0	DCCA Discard(Bytes):	0
DCCA Discard(Pkts):	0	DCCA Discard(Pkts):	0
No Rule Match(Bytes):	0	No Rule Match(Bytes):	0
No Rule Match(Pkts):	0	No Rule Match(Pkts):	0
ICAP(Bytes):	0	ICAP(Bytes):	N/A
ICAP(Pkts):	0	ICAP(Pkts):	N/A
SFW(Bytes):	0	SFW(Bytes):	0
SFW(Pkts):	0	SFW(Pkts):	0
Hierarchical ENF(Bytes):	0	Hierarchical ENF(Bytes):	0
Hierarchical ENF(Pkts):	0	Hierarchical ENF(Pkts):	0
Dynamic CA Gate(Bytes):	0	Dynamic CA Gate(Bytes):	:
Dynamic CA Gate(Pkts):	0	Dynamic CA Gate(Pkts):	0
NAT64 Cancel(Bytes):	0	NAT64 Cancel(Bytes):	0
NAT64 Cancel(Pkts):	0	NAT64 Cancel(Pkts):	0
Bearer Not Found(Bytes):	0	Bearer Not Found(Bytes):	0
Bearer Not Found(Pkts):	0	Bearer Not Found(Pkts):	0


```

.
.
QCI 9:
  Bearer Active:                0   Bearer setup:                0
  Bearer Released:              0   Bearer Rejected:            0

  Uplink Bytes forwarded:       0   Downlink Bytes forwarded:   0
  Uplink Pkts forwarded:        0   Downlink Pkts forwarded:    0
  Uplink Bytes dropped:          0   Downlink Bytes dropped:     0
  Uplink Pkts dropped:           0   Downlink Pkts dropped:      0

```

show configuration

The output of this command has been enhanced to show the Stats Profile configuration settings.

- stats-profile <stats_profile_name>
- qci <qci number> arp <arp number>
- packet-drop (*if packet-drop is enabled*)

show stats-profile name

This new command in *Exec Mode* shows the configuration settings for the specified Stats Profile.

- Stats Profile Name: <stats_profile_name>
- qci <qci number> arp <arp_number(s)>
- packet-drop <if packet drop is enabled>

DSCP Marking Based on Both QCI and ARP Values

Feature Description

P-GW allows users to perform DSCP marking based on QoS Class Identifier (QCI) values. This functionality has been expanded to include the Priority Level (PL) values 1-15 of Allocation and Retention Priority (ARP), which allows users to assign different DSCP values for bearers with the same QCI but different ARP priority values. For example, the ability to assign DSCP values based on QCI+ARP could be used to meet compliance on priority and emergency calling via VoLTE.

Applies to the P-GW for the following interfaces:

- S5
- S8
- SGi
- S2b

Applies to the S-GW for the following interfaces:

- S1-U
- S5

- S8
- S11
- S4

Relationships to Other Features

ECS populates the DSCP values in inner IP header. These values are fetched from the DSCP table by means of a sessmanager API. Since DSCP values are now available for QCI-ARP combination, the API is replaced by a wrapper API that will accept both QCI and ARP and provide the DSCP values to ECS in a new data structure.

The API will return correct values in the following scenarios:

- 1 QCI-DSCP table is not configured, or it is not associated for this session.
API will return an indication to ECS that table was not found.
- 2 Table is configured, but entry for the given QCI value is not present in the table.
API will not populate the structure and keep the same unaltered.
- 3 Entry for given QCI is present, but it is not available for the given QCI-ARP pair.
The default DSCP values for that particular QCI will be populated in the return structure.
- 4 Entry for given QCI-ARP combination is present.
The DSCP values for given QCI-ARP combination will be populated in the return structure.

Once values are received from SM, ECS caches these values and uses the cached values for marking the further packets. Another lookup into the table is done only when there is a mismatch between the currently cached QCI-ARP value and the current packet's QCI-ARP value. Therefore, any change in the QCI-ARP table would be affected for inner DSCP marking on existing flows only in case of QCI or ARP change.

Licensing

DSCP marking capability requires that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

The expansion of functionality to allow assigning different DSCP values for bearers with the same QCI, but different APR values, works as follows.

- DSCP marking of packets based on QCI+ARP combination allowed
- QCI + ARP configuration will override any DSCP entry for that QCI+ARP combination
- QCI only DSCP entry will override all existing QCI+ARP configuration
- Applying associated DSCP marking for QCI+ARP for Uplink and Downlink functionality is also allowed

Configuring DSCP Marking Based on Both QCI and ARP Values

This section describes how to configure DSCP marking based on both QCI and ARP values.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI and ARP values to enforceable Quality of Service (QoS) parameters:

```
configure
  qci-qos-mapping name
    qci num [ arp-priority-level arp_value ] [ downlink | encaps-header { copy-inner | dscp-marking
dscp-marking-value } ] [ internal-qos priority priority ] [ user-datagram dscp-marking dscp-marking-value
] [ uplink | downlink ] [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ] [
internal-qos priority priority ] [ user-datagram dscp-marking dscp-marking-value ] ]
  end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.
QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values. In addition, QCI values 65, 66, 69, and 70 can be used in StarOS release 21.0 and later.
From 3GPP Release 8 onwards, operator-specific/non-standard QCIs are supported and carriers can define QCI 128- 254.
- **arp-priority-level arp_value**: Specifies the address retention priority (ARP) priority level.
arp_value must be an integer from 1 through 15.
- The above configuration only shows one keyword example. Refer to the *QCI - QoS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Use the following example to disable QCI and ARP values:

```
configure
  qci-qos-mapping name
    no qci num [ arp-priority-level arp_value ]
  end
```

Associating QCI-QoS Mapping Configuration

Use the following example to specify that the P-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
  context context_name
    pgw-service pgw_service_name
      associate qci-qos-mapping name
    end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Use the following example to specify that the S-GW service is to be associated with an existing QCI-QoS mapping configuration:

```
configure
  context context_name
    sgw-service sgw_service_name
      associate qci-qos-mapping name
    end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context.

Configuring CS5 Marking for GTP-C

Use the following example to mark DSCP precedence CS5 on control packets:

```
configure
  context context_name
    ggsn-service ggsn_service_name
      ip qos-dscp gtpc cs5
    end
```

Notes:

- Designates Class Selector 5 DSCP precedence for GTP-C packets.

Verifying the Configuration

Use the following command in Exec mode to display/verify the configuration.

```
show configuration
```

Monitoring DSCP Marking Based on Both QCI and ARP Values

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of DSCP marking based on both QCI and ARP values.

show qci-qos-mapping table all

The output of this command has been enhanced to show the ARP value:

- arp-priority-level

New Standard QCI Support

CDETS: CSCuy20910 - Support of new standard QCIs (65, 66, 69, 70)

Applicable Products: P-GW, SAEGW, S-GW

Feature Description

The P-GW/SAEGW/S-GW support additional new 3GPP-defined standard QCIs. QCIs 65, 66, 69, and 70 are now supported for Mission Critical and Push-to-Talk (MCPTT) applications. These new standard QCIs are supported in addition to the previously supported QCIs of 1 through 9, and operator-defined QCIs 128 through 254.

The StarOS will continue to reject QCIs 10 through 127 sent by the PCRF.

Licensing



Important

New Standard QCI Support is a licensed feature. Contact your Cisco account or support representative for licensing details.

How it Works

Although the 3GPP specification mentions that only QCIs 65 and 69 can co-exist, there is no hard restriction on the QCIs in the StarOS implementation of this feature, as that is applicable to the PCRF. The P-GW acts as a pass-through node and allows QCIs 65 and 69 if a different QCI combination is requested from PCRF.

With support for standard QCIs 65, 66, 69, and 70 present, the implementation has also added support across the following StarOS interfaces:

- **Gx:** Gx processes Default Bearer QoS and Rule Validation allowing the new Mission Critical (MC)/Push to Talk (PTT) QCIs. When the MC/PTT bit is not negotiated with the PCRF, the PCEF will reject the creation of a bearer or reject call setup.
- **sessmgr:** The P-GW sessmgr now processes the updating and modification of QoS. The P-GW rejects all UE initiated BRC creation for the new standard QCIs.
- **ECS:** ECS accepts the new standard QCIs when received from the PCRF and will reject them when either the license is not configured or the same is received in 3G. The ECS is able to update a Default bearer with this QoS change or create a Dedicated Bearer for the new standard QCIs.

Handoff Behavior

For Gn/Gp handoffs, local mapping via the CLI is supported so that the P-GW/SAEGW/S-GW is in sync with the MME-to-SGSN context transfer. The following scenarios are supported:

No Local QoS Mapping Present: When no local mapping is present for the new QCIs, a call handoff from 4G to 3G will be rejected.

Local QoS Mapping Present: Three scenarios are supported when local mapping is present:

- **Local Mapping present for MME-SGSN and PCRF Out of Synchronization:** When local mapping is present it is assumed that the QoS mapping in the P-GW is in sync with the mapping from the MME to SGSN. Even if the QoS mapping for one of the transferred PDPs during a Gn/Gp handoff is not in sync with MME-SGSN mapping, the P-GW/SAEGW/S-GW still continues with the handoff with the local mapping present. However, the CDR generated while waiting for the PCRF response during the handoff would be out of sync with the CDR's received after the handoff.

- **Mapping present for MME-SGSN and PCRF in Synchronization:** When local mapping is in sync with the MME-SGSN there is no difference in the CDR generated after the handoff.
- **Partial Mapping Present:** Partial mapping occurs when some MC/PTT QCI(s) have mapping and the remainder of the MC/PTT QCI(s) do not have mapping. In this case the call is dropped.

Expected Call Flow Output

This section provides detailed information on the expected call flow output for various scenarios with the New Standard QCI support feature:

- New Call Procedure
- Handoff Procedures
- UE Initiated Bearer Creation
- Bearer Creation
- Bearer Update

These sections describe new behaviors and provide behavior clarification for this feature. Behavior not described is similar to that for Standard QCIs.

New Call Procedure

This section provides detailed information on the expected call flow output for various new call procedure scenarios with the New Standard QCI Support feature.

Table 21: Expected Call Flow Output: New Call Procedure

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Setup 3G (GGSN)	N/A	N/A	Create PDP Req	Std QCI	Enabled	MC/PTT- Std QCI	N/A	N/A	Call rejected by application
Setup eHRPD	N/A	N/A	PBU	Std QCI	Enabled	MC/PTT- Std QCI	N/A	N/A	Call accepted and created with this rule
Setup 4G (RAT: S4-SGSN)	N/A	N/A	Create Session Req	Std QCI	Enabled	MC/PTT- Std QCI	N/A	N/A	Call accepted and created with this rule

Handoff Procedures

This section provides detailed information on expected call flow output for various handoff procedure scenarios with the New Standard QCI Support feature.

Table 22: Expected Call Flow Output: Handoff Procedures

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
Default bearer existing for WiFi	Call existing with MC/PTT- QCI requested to handoff to MC/PTT- QCI	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT- Std QCI received for default bearer	N/A	Handoff accepted and down MC/PTT Std QCI applied	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GnGp Handoff (4G (LTE) to 3G (GGSN))	Update PDP request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT- QCI requested to Std-QCI where mapping not received for few MC/PTT- QCI bearers	Update PDP Req	Partial mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	Partial mapped Std QCI for MC/PTT- QCIs received. Here mapping is not Received for some PDP bearers .	N/A	Handoff rejected and call drop Initiated
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT- QCI requested to Std-QCI where no mapping received for few MC/PTT- QCI bearers	Update PDP Req	No mapping Received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	No mapping received	N/A	Handoff rejected and call drop initiated
	Update PDP request received for primary PDP and pending response (No-Local Mapping Present)	Call existing with Std primary PDP & MC/PTT- QCI requested to Std-QCI	Update PDP Req	N/A	Enabled	N/A	MC/PTT update rules received for Std QCI dedicated bearers	N/A	MC/PTT QCI mapped rule associated dedicated bearer purged and handoff accepted
		Call existing with MC/PTT primary PDP	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response (No-local mapping present)								Handoff rejected and call drop Initiated (dropped before Initiating CCA-U for handoff)
	Update PDP Request received for primary PDP and pending response (Local mapping present)	Call existing with MC/PTT- QCI requested to Std-QCI	Update PDP Req	PCRF Timeout No Response received	Enabled	N/A	No response from PCRF / CCA-U timeout	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and same as what QCI values comes in UPC during HO)	Call existing with MC/PTT- QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT- QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
			Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is mixed. (Local mapping present and not same as what QCI values comes in UPC during HO).	Call existing with MC/PTT-QCI requested to Std-QCI							
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and same as what QCI values come in UPC during HO)	Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT-QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted
		Call existing with MC/PTT-QCI requested to Std-QCI	Update PDP Req	Mapping received from PCRF for MC/PTT-QCI to Std-QCI	Enabled	N/A	All mapping received from PCRF	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
	Update PDP Request received for primary PDP and pending response. BCM mode is UE Only. (Local mapping present and not same as what QCI values come in UPC during HO.)								
	Update PDP Request received for primary PDP and pending response (Local mapping present/not present)	Call existing with MC/PTT- QCI requested to Std-QCI. Also suppress- NRUPC UPC is configured at the GGSN service level.	Update PDP Req	N/A	Enabled	N/A	N/A	N/A	Handoff rejected and call drop initiated
	Update PDP Request received for primary PDP and response sent (Local mapping present)		Update PDP Req	Complete mapping Received from PCRF for MC/PTT- QCI to Std-QCI (as per Local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT- QCI	N/A	Handoff accepted

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
		Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers							
	Update PDP Request received for primary PDP and response sent (Local mapping present)	Call existing with MC/PTT-QCI requested to Std-QCI mapping received for All MC/PTT-QCI bearers	Update PDP Req	Complete mapping received from PCRF for MC/PTT-QCI to Std-QCI (different from local MC/PTT to Std QCI mapping)	Enabled	N/A	All mapped Std QCI for MC/PTT-QCI	N/A	Handoff accepted and Update PDP Response sent for all bearers
eHRPD -> LTE	Create Session Req received with ho_ind = 1	Only one bearer existing with the call	Create Session Req	MC/PTT - QCI	Enabled	N/A	MC/PTT-Std QCI received with rules	N/A	Handoff accepted and dedicated bearer are created with the MC/PTT-Std QCI received.
LTE -> eHRPD	Default + dedicated bearer existing for LTE	Call existing with MC/PTT-QCI	PBU	N/A	Enabled	N/A	N/A	N/A	Handoff accepted and PBA is sent and dedicated bearer rules are added under single bearer

UE Initiated Bearer Creation

This section provides detailed information on the expected call flow output for various UE initiated bearer creation scenarios with the New Standard QCI Support feature.

Table 23: Expected Call Flow Output: UE Initiated Bearer Creation

Procedure (3G/4G/S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
LTE UE Initiated Bearer	Default bearer existing for LTE	N/A	Bearer Resource Command	MC/PTT- Std QCI	N/A	N/A	N/A	N/A	BRC rejected by application
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Disabled	N/A	MC/PTT- Std dedicated QCI	N/A	BRC rejected / rule rejected with resource allocation failure
	Default bearer existing for LTE	N/A	Bearer Resource Command	Std QCI	Enabled	N/A	MC/PTT- Std dedicated QCI	N/A	BRC rejected /CBReq initiated with MC/PTT- Std QCI

Bearer Creation

This section provides detailed information on the expected call flow output for Bearer Creation scenarios with the New Standard QCI Support feature.

Table 24: Expected Call Flow Output: Bearer Creation

Procedure (3G/4G/S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN secondary PDP creation	Primary PDP existing for GGSN	New secondary PDP requested with MC/PTT-Std-QCI	RAR Procedure	N/A	Enabled	N/A	N/A	Rules received with MC/PTT-Std QCI	CCR-I resource allocation failure for secondary PDP sent to PCRF

Bearer Update

This section provides detailed information on the expected call flow output for Bearer Update scenarios with the New Standard QCI Support feature.

Table 25: Expected Call Flow Output: Bearer Update

Procedure (3G/4G/ S2b/S2a)	Pre-Condition	Call QCI Modification	Message Type	Request with Type Of QCI	PGW License	Gx Interface (Type of Re-mapped QCI received)			Expected Behavior
						CCA-I	CCA-U	RAR	
GGSN Primary PDP QoS modification	Primary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT- Std QCI modification	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MCPTT- Std QCI for primary PDP received	CCR-I QoS modification failure for primary PDP QoS modification rejected
GGSN Secondary PDP QoS Modification	Primary PDP & secondary PDP existing for GGSN	Call existing with Std-QCI requested to MC/PTT- Std QCI modification for secondary PDP	RAR Procedure	MC/PTT- Std QCI	Enabled	N/A	N/A	MCPTT- Std QCI for secondary PDP with rules received	CCR-I resource allocation failure for secondary PDP QoS modification sent

Configuring New Standard QCIs

Configuring New Standard QCIs consists of the following tasks:

- Configuring QCI-QoS Mapping
- Configuring Local Mapping for Gn/Gp Support
- Configuring Transaction Rate Network Initiated Setup/Teardown Events
- Enable Mission Critical QCIs

Configuring QCI-QoS Mapping

Standard QCI options **65**, **66**, **69**, and **70** have been added to the **qci** command in *QCI-QoS Mapping Configuration Mode*.

To configure QCI-QoS Mapping for new standard QCIs:

```
configure
qci-qos-mapping qci_qos_map_name
qci { 1-9 | 65 | 66 | 69 | 70 }
end
```

To disable new QCI-QoS mapping for new standard QCIs:

```
configure
qci-qos-mapping qci_qos_map_name
no qci { 1-9 | 65 | 66 | 69 | 70 }
end
```

Notes:

- **qci** options 65 and 66 are available for guaranteed bit rate (GBR) network initiated QCI values only.
- **qci** options 69 and 70 are available for non-GBR network initiated QCI values only.
- **no** disables the specified standard **qci** value.

Configuring Local QCI Mapping for Gn/Gp QoS Support

Use the following example to configure local QCI mapping for Gn/Gp support:

```
configure
qci-qos-mapping mapping_name
qci { 1-9 | 65 | 66 | 69 | 70 } pre-rel8-qos-mapping qci_value
end
```

Notes:

- **qci**: When the MPS license is disabled, this value must be a Standard QoS Class Identifier (QCI) from 1 to 9. When the MPS license is enabled, this value must be a Standard QCI from 1 to 9, or 65, 66, 69, 70.
- **qci** 65 and 66 are Mission Critical/Push to Talk (MC/PTT) GBR values and values 69 and 70 are MC/PTT Non-GBR values.
- **qci** values 65 and 66 can only be mapped to QCI values 1 through 4, and QCI values 69 and 70 can only be mapped to QCI values 5 through 9.

Configuring Transaction Rate Network Initiated Setup/Teardown Events

To configure transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
transaction-rate nw-initiated-setup-teardown-events qci { 1-9 | 65 | 66 | 69 | 70 | 128-254 }
end
```

To disable transaction rate network initiated setup/teardown events for new standard QCI values:

```
configure
no transaction-rate nw-initiated-setup-teardown-events qci qci_value
end
```

Notes:

- **65** and **66** are available options for GBR network-initiated QCI values.
- **69** and **70** are available options for non-GBR network-initiated QCI values.

- **no** disables transaction rate network initiated setup/teardown events for the specified new standard QCI value.

Enable Mission Critical QCIs

The **mission-critical-qcis** keyword in the **diameter encode-supported-features** command is required for support between the PCEF and PCRF for new standard QCI support. Use the following example to enable mission critical QCIs in *Policy Control Configuration Mode*:

```
configure
context context_name
  ims-auth-service ims-ggsn-auth
  policy-control
    diameter encode-supported-features mission-critical-qcis
  end
```

To disable this feature, enter the following commands:

```
configure
context context_name
  ims-auth-service ims-ggsn-auth
  policy-control
    no diameter encode-supported-features
  end
```

Notes:



Important

The LTE Wireless Priority Feature Set must be enabled to configure the **mission-critical-qcis** option. The LTE Wireless Priority Feature Set is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

Verifying the Configuration

Use the following example to verify the new standard QCI configuration:

```
show qci-qos-mapping table name qci_qos_mapping_table_name
```

Notes:

- The command output provides all qci-qos mapping attributes, including the new standard qci number. If any of the attributes are incorrect, repeat the configuration procedure in this chapter to correct the settings.

Monitoring the Feature

This section describes how to monitor the New Standard QCI Support feature.

Bulk Statistics

This section lists the bulk statistics that have been added to support the New Standard QCIs feature.

APN Schema

The following bulk statistics have been added to the APN Schema to support the New Standard QCIs feature.

```

qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66

```

```

sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70

```

GTPU Schema

The following bulk statistics have been added to the GTPU Schema to support the New Standard QCIs feature.

```

qci65-uplink-pkts
qci65-uplink-bytes
qci65-dwlink-pkts
qci65-dwlink-byte
qci65-pkts-discard
qci65-bytes-discard
qci66-uplink-pkts
qci66-uplink-bytes
qci66-dwlink-pkts
qci66-dwlink-byte
qci66-pkts-discard
qci66-bytes-discard
qci69-uplink-pkts
qci69-uplink-bytes
qci69-dwlink-pkts
qci69-dwlink-byte
qci69-pkts-discard
qci69-bytes-discard
qci70-uplink-pkts
qci70-uplink-bytes
qci70-dwlink-pkts
qci70-dwlink-byte
qci70-pkts-discard
qci70-bytes-discard

```

P-GW Schema

The following bulk statistics have been added to the P-GW schema to support the New Standard QCIs feature.

```

subgosstat-bearact-qci65
subgosstat-bearact-qci66
subgosstat-bearact-qci69
subgosstat-bearact-qci70
subgosstat-bearsetup-qci65
subgosstat-bearsetup-qci66
subgosstat-bearsetup-qci69
subgosstat-bearsetup-qci70
subgosstat-bearrel-qci65
subgosstat-bearrel-qci66
subgosstat-bearrel-qci69
subgosstat-bearrel-qci70
subdatastat-uppktfwd-qci65
subdatastat-uppktfwd-qci66
subdatastat-uppktfwd-qci69
subdatastat-uppktfwd-qci70
subdatastat-upbytefwd-qci65
subdatastat-upbytefwd-qci66
subdatastat-upbytefwd-qci69
subdatastat-upbytefwd-qci70
subdatastat-downpktfwd-qci65
subdatastat-downpktfwd-qci66
subdatastat-downpktfwd-qci69
subdatastat-downpktfwd-qci70
subdatastat-downbytefwd-qci65
subdatastat-downbytefwd-qci66
subdatastat-downbytefwd-qci69
subdatastat-downbytefwd-qci70
subdatastat-uppktdrop-qci65
subdatastat-uppktdrop-qci66
subdatastat-uppktdrop-qci69
subdatastat-uppktdrop-qci70
subdatastat-upbytedrop-qci65

```

```

subdatastat-upbytedrop-qci66
subdatastat-upbytedrop-qci69
subdatastat-upbytedrop-qci70
subdatastat-downpktdrop-qci65
subdatastat-downpktdrop-qci66
subdatastat-downpktdrop-qci69
subdatastat-downpktdrop-qci70
subdatastat-downbytedrop-qci65
subdatastat-downbytedrop-qci66
subdatastat-downbytedrop-qci69
subdatastat-downbytedrop-qci70
subdatastat-uppktdropmbrexc-qci65
subdatastat-uppktdropmbrexc-qci66
subdatastat-uppktdropmbrexc-qci69
subdatastat-uppktdropmbrexc-qci70
subdatastat-upbytedropmbrexc-qci65
subdatastat-upbytedropmbrexc-qci66
subdatastat-upbytedropmbrexc-qci69
subdatastat-upbytedropmbrexc-qci70
subdatastat-downpktdropmbrexc-qci65
subdatastat-downpktdropmbrexc-qci66
subdatastat-downpktdropmbrexc-qci69
subdatastat-downpktdropmbrexc-qci70
subdatastat-downbytedropmbrexc-qci65
subdatastat-downbytedropmbrexc-qci66
subdatastat-downbytedropmbrexc-qci69
subdatastat-downbytedropmbrexc-qci70

```

SAEGW Schema

The following bulk statistics have been added to the SAEGW Schema to support the New Standard QCIs feature.

```

sgw-totepsbearact-qci65
sgw-totepsbearact-qci66
sgw-totepsbearact-qci69
sgw-totepsbearact-qci70
sgw-totepsbearset-qci65
sgw-totepsbearset-qci66
sgw-totepsbearset-qci69
sgw-totepsbearset-qci70
sgw-totepsbearrel-qci65
sgw-totepsbearrel-qci66
sgw-totepsbearrel-qci69
sgw-totepsbearrel-qci70
sgw-totepsbearmod-qci65
sgw-totepsbearmod-qci66
sgw-totepsbearmod-qci69
sgw-totepsbearmod-qci70
sgw-totepsbearrel-dedrsn-pgw-qci65
sgw-totepsbearrel-dedrsn-pgw-qci66
sgw-totepsbearrel-dedrsn-pgw-qci69
sgw-totepsbearrel-dedrsn-pgw-qci70
sgw-totepsbearrel-dedrsn-slerr-qci65
sgw-totepsbearrel-dedrsn-slerr-qci66
sgw-totepsbearrel-dedrsn-slerr-qci69
sgw-totepsbearrel-dedrsn-slerr-qci70
sgw-totepsbearrel-dedrsn-s5err-qci65
sgw-totepsbearrel-dedrsn-s5err-qci66
sgw-totepsbearrel-dedrsn-s5err-qci69
sgw-totepsbearrel-dedrsn-s5err-qci70
sgw-totepsbearrel-dedrsn-s4err-qci65
sgw-totepsbearrel-dedrsn-s4err-qci66
sgw-totepsbearrel-dedrsn-s4err-qci69
sgw-totepsbearrel-dedrsn-s4err-qci70
sgw-totepsbearrel-dedrsn-sl2err-qci65
sgw-totepsbearrel-dedrsn-sl2err-qci66
sgw-totepsbearrel-dedrsn-sl2err-qci69
sgw-totepsbearrel-dedrsn-sl2err-qci70
sgw-totepsbearrel-dedrsn-local-qci65
sgw-totepsbearrel-dedrsn-local-qci66

```

```

sgw-totepsbearrel-dedrsn-local-qci69
sgw-totepsbearrel-dedrsn-local-qci70
sgw-totepsbearrel-dedrsn-pdn-qci65
sgw-totepsbearrel-dedrsn-pdn-qci66
sgw-totepsbearrel-dedrsn-pdn-qci69
sgw-totepsbearrel-dedrsn-pdn-qci70
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-qci70
sgw-totepsbearrel-dedrsn-pathfail-s11-qci65
sgw-totepsbearrel-dedrsn-pathfail-s11-qci66
sgw-totepsbearrel-dedrsn-pathfail-s11-qci69
sgw-totepsbearrel-dedrsn-pathfail-s11-qci70
sgw-totepsbearrel-dedrsn-pathfail-s12-qci65
sgw-totepsbearrel-dedrsn-pathfail-s12-qci66
sgw-totepsbearrel-dedrsn-pathfail-s12-qci69
sgw-totepsbearrel-dedrsn-pathfail-s12-qci70
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci70
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci65
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci66
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci69
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci70
sgw-totepsbearrel-dedrsn-other-qci65
sgw-totepsbearrel-dedrsn-other-qci66
sgw-totepsbearrel-dedrsn-other-qci69
sgw-totepsbearrel-dedrsn-other-qci70
sgw-datastat-ul-qci65totbyte
sgw-datastat-ul-qci65totpkt
sgw-datastat-ul-qci66totbyte
sgw-datastat-ul-qci66totpkt
sgw-datastat-ul-qci69totbyte
sgw-datastat-ul-qci69totpkt
sgw-datastat-ul-qci70totbyte
sgw-datastat-ul-qci70totpkt
sgw-datastat-ul-dropstat-qci65totbyte
sgw-datastat-ul-dropstat-qci65totpkt
sgw-datastat-ul-dropstat-qci66totbyte
sgw-datastat-ul-dropstat-qci66totpkt
sgw-datastat-ul-dropstat-qci69totbyte
sgw-datastat-ul-dropstat-qci69totpkt
sgw-datastat-ul-dropstat-qci70totbyte
sgw-datastat-ul-dropstat-qci70totpkt
sgw-datastat-dl-qci65totbyte
sgw-datastat-dl-qci65totpkt
sgw-datastat-dl-qci66totbyte
sgw-datastat-dl-qci66totpkt
sgw-datastat-dl-qci69totbyte
sgw-datastat-dl-qci69totpkt
sgw-datastat-dl-qci70totbyte
sgw-datastat-dl-qci70totpkt
sgw-datastat-dl-dropstat-qci65totbyte
sgw-datastat-dl-dropstat-qci65totpkt
sgw-datastat-dl-dropstat-qci66totbyte
sgw-datastat-dl-dropstat-qci66totpkt
sgw-datastat-dl-dropstat-qci69totbyte
sgw-datastat-dl-dropstat-qci69totpkt
sgw-datastat-dl-dropstat-qci70totbyte
sgw-datastat-dl-dropstat-qci70totpkt
sgw-slu-ul-qci65totbyte
sgw-slu-ul-qci65totpkt
sgw-slu-ul-qci66totbyte

```

```

sgw-slu-ul-qci66totpkt
sgw-slu-ul-qci69totbyte
sgw-slu-ul-qci69totpkt
sgw-slu-ul-qci70totbyte
sgw-slu-ul-qci70totpkt
sgw-slu-ul-drop-qci65totbyte
sgw-slu-ul-drop-qci65totpkt
sgw-slu-ul-drop-qci66totbyte
sgw-slu-ul-drop-qci66totpkt
sgw-slu-ul-drop-qci69totbyte
sgw-slu-ul-drop-qci69totpkt
sgw-slu-ul-drop-qci70totbyte
sgw-slu-ul-drop-qci70totpkt
sgw-slu-dl-qci65totbyte
sgw-slu-dl-qci65totpkt
sgw-slu-dl-qci66totbyte
sgw-slu-dl-qci66totpkt
sgw-slu-dl-qci69totbyte
sgw-slu-dl-qci69totpkt
sgw-slu-dl-qci70totbyte
sgw-slu-dl-qci70totpkt
sgw-slu-dl-drop-qci65totbyte
sgw-slu-dl-drop-qci65totpkt
sgw-slu-dl-drop-qci66totbyte
sgw-slu-dl-drop-qci66totpkt
sgw-slu-dl-drop-qci69totbyte
sgw-slu-dl-drop-qci69totpkt
sgw-slu-dl-drop-qci70totbyte
sgw-slu-dl-drop-qci70totpkt
sgw-s4u-ul-qci65totbyte
sgw-s4u-ul-qci65totpkt
sgw-s4u-ul-qci66totbyte
sgw-s4u-ul-qci66totpkt
sgw-s4u-ul-qci69totbyte
sgw-s4u-ul-qci69totpkt
sgw-s4u-ul-qci70totbyte
sgw-s4u-ul-qci70totpkt
sgw-s4u-ul-drop-qci65totbyte
sgw-s4u-ul-drop-qci65totpkt
sgw-s4u-ul-drop-qci66totbyte
sgw-s4u-ul-drop-qci66totpkt
sgw-s4u-ul-drop-qci69totbyte
sgw-s4u-ul-drop-qci69totpkt
sgw-s4u-ul-drop-qci70totbyte
sgw-s4u-ul-drop-qci70totpkt
sgw-s4u-dl-qci65totbyte
sgw-s4u-dl-qci65totpkt
sgw-s4u-dl-qci66totbyte
sgw-s4u-dl-qci66totpkt
sgw-s4u-dl-qci69totbyte
sgw-s4u-dl-qci69totpkt
sgw-s4u-dl-qci70totbyte
sgw-s4u-dl-qci70totpkt
sgw-s4u-dl-drop-qci65totbyte
sgw-s4u-dl-drop-qci65totpkt
sgw-s4u-dl-drop-qci66totbyte
sgw-s4u-dl-drop-qci66totpkt
sgw-s4u-dl-drop-qci69totbyte
sgw-s4u-dl-drop-qci69totpkt
sgw-s4u-dl-drop-qci70totbyte
sgw-s4u-dl-drop-qci70totpkt
sgw-s12-ul-qci65totbyte
sgw-s12-ul-qci65totpkt
sgw-s12-ul-qci66totbyte
sgw-s12-ul-qci66totpkt
sgw-s12-ul-qci69totbyte
sgw-s12-ul-qci69totpkt
sgw-s12-ul-qci70totbyte
sgw-s12-ul-qci70totpkt
sgw-s12-ul-drop-qci65totbyte
sgw-s12-ul-drop-qci65totpkt
sgw-s12-ul-drop-qci66totbyte
sgw-s12-ul-drop-qci66totpkt

```

```

sgw-s12-ul-drop-qci69totbyte
sgw-s12-ul-drop-qci69totpkt
sgw-s12-ul-drop-qci70totbyte
sgw-s12-ul-drop-qci70totpkt
sgw-s12-dl-qci65totbyte
sgw-s12-dl-qci65totpkt
sgw-s12-dl-qci66totbyte
sgw-s12-dl-qci66totpkt
sgw-s12-dl-qci69totbyte
sgw-s12-dl-qci69totpkt
sgw-s12-dl-qci70totbyte
sgw-s12-dl-qci70totpkt
sgw-s12-dl-drop-qci65totbyte
sgw-s12-dl-drop-qci65totpkt
sgw-s12-dl-drop-qci66totbyte
sgw-s12-dl-drop-qci66totpkt
sgw-s12-dl-drop-qci69totbyte
sgw-s12-dl-drop-qci69totpkt
sgw-s12-dl-drop-qci70totbyte
sgw-s12-dl-drop-qci70totpkt
sgw-s5-ul-qci65totbyte
sgw-s5-ul-qci65totpkt
sgw-s5-ul-qci66totbyte
sgw-s5-ul-qci66totpkt
sgw-s5-ul-qci69totbyte
sgw-s5-ul-qci69totpkt
sgw-s5-ul-qci70totbyte
sgw-s5-ul-qci70totpkt
sgw-s5-ul-drop-qci65totbyte
sgw-s5-ul-drop-qci65totpkt
sgw-s5-ul-drop-qci66totbyte
sgw-s5-ul-drop-qci66totpkt
sgw-s5-ul-drop-qci69totbyte
sgw-s5-ul-drop-qci69totpkt
sgw-s5-ul-drop-qci70totbyte
sgw-s5-ul-drop-qci70totpkt
sgw-s5-dl-qci65totbyte
sgw-s5-dl-qci65totpkt
sgw-s5-dl-qci66totbyte
sgw-s5-dl-qci66totpkt
sgw-s5-dl-qci69totbyte
sgw-s5-dl-qci69totpkt
sgw-s5-dl-qci70totbyte
sgw-s5-dl-qci70totpkt
sgw-s5-dl-drop-qci65totbyte
sgw-s5-dl-drop-qci65totpkt
sgw-s5-dl-drop-qci66totbyte
sgw-s5-dl-drop-qci66totpkt
sgw-s5-dl-drop-qci69totbyte
sgw-s5-dl-drop-qci69totpkt
sgw-s5-dl-drop-qci70totbyte
sgw-s5-dl-drop-qci70totpkt
sgw-s8-ul-qci65totbyte
sgw-s8-ul-qci65totpkt
sgw-s8-ul-qci66totbyte
sgw-s8-ul-qci66totpkt
sgw-s8-ul-qci69totbyte
sgw-s8-ul-qci69totpkt
sgw-s8-ul-qci70totbyte
sgw-s8-ul-qci70totpkt
sgw-s8-ul-drop-qci65totbyte
sgw-s8-ul-drop-qci65totpkt
sgw-s8-ul-drop-qci66totbyte
sgw-s8-ul-drop-qci66totpkt
sgw-s8-ul-drop-qci69totbyte
sgw-s8-ul-drop-qci69totpkt
sgw-s8-ul-drop-qci70totbyte
sgw-s8-ul-drop-qci70totpkt
sgw-s8-dl-qci65totbyte
sgw-s8-dl-qci65totpkt
sgw-s8-dl-qci66totbyte
sgw-s8-dl-qci66totpkt
sgw-s8-dl-qci69totbyte

```

```

sgw-s8-dl-qci69totpkt
sgw-s8-dl-qci70totbyte
sgw-s8-dl-qci70totpkt
sgw-s8-dl-drop-qci65totbyte
sgw-s8-dl-drop-qci65totpkt
sgw-s8-dl-drop-qci66totbyte
sgw-s8-dl-drop-qci66totpkt
sgw-s8-dl-drop-qci69totbyte
sgw-s8-dl-drop-qci69totpkt
sgw-s8-dl-drop-qci70totbyte
sgw-s8-dl-drop-qci70totpkt
sgw-s5s8-ul-qci65totbyte
sgw-s5s8-ul-qci65totpkt
sgw-s5s8-ul-qci66totbyte
sgw-s5s8-ul-qci66totpkt
sgw-s5s8-ul-qci69totbyte
sgw-s5s8-ul-qci69totpkt
sgw-s5s8-ul-qci70totbyte
sgw-s5s8-ul-qci70totpkt
sgw-s5s8-ul-drop-qci65totbyte
sgw-s5s8-ul-drop-qci65totpkt
sgw-s5s8-ul-drop-qci66totbyte
sgw-s5s8-ul-drop-qci66totpkt
sgw-s5s8-ul-drop-qci69totbyte
sgw-s5s8-ul-drop-qci69totpkt
sgw-s5s8-ul-drop-qci70totbyte
sgw-s5s8-ul-drop-qci70totpkt
sgw-s5s8-dl-qci65totbyte
sgw-s5s8-dl-qci65totpkt
sgw-s5s8-dl-qci66totbyte
sgw-s5s8-dl-qci66totpkt
sgw-s5s8-dl-qci69totbyte
sgw-s5s8-dl-qci69totpkt
sgw-s5s8-dl-qci70totbyte
sgw-s5s8-dl-qci70totpkt
sgw-s5s8-dl-drop-qci65totbyte
sgw-s5s8-dl-drop-qci65totpkt
sgw-s5s8-dl-drop-qci66totbyte
sgw-s5s8-dl-drop-qci66totpkt
sgw-s5s8-dl-drop-qci69totbyte
sgw-s5s8-dl-drop-qci69totpkt
sgw-s5s8-dl-drop-qci70totbyte
sgw-s5s8-dl-drop-qci70totpkt
pgw-subqosstat-bearact-qci65
pgw-subqosstat-bearact-qci66
pgw-subqosstat-bearact-qci69
pgw-subqosstat-bearact-qci70
pgw-subqosstat-bearset-qci65
pgw-subqosstat-bearset-qci66
pgw-subqosstat-bearset-qci69
pgw-subqosstat-bearset-qci70
pgw-subqosstat-bearrel-qci65
pgw-subqosstat-bearrel-qci66
pgw-subqosstat-bearrel-qci69
pgw-subqosstat-bearrel-qci70
pgw-subdatastat-ulpktfwd-qci65
pgw-subdatastat-ulpktfwd-qci66
pgw-subdatastat-ulpktfwd-qci69
pgw-subdatastat-ulpktfwd-qci70
pgw-subdatastat-ulbytefwd-qci65
pgw-subdatastat-ulbytefwd-qci66
pgw-subdatastat-ulbytefwd-qci69
pgw-subdatastat-ulbytefwd-qci70
pgw-subdatastat-dlpktfwd-qci65
pgw-subdatastat-dlpktfwd-qci66
pgw-subdatastat-dlpktfwd-qci69
pgw-subdatastat-dlpktfwd-qci70
pgw-subdatastat-dlbytefwd-qci65
pgw-subdatastat-dlbytefwd-qci66
pgw-subdatastat-dlbytefwd-qci69
pgw-subdatastat-dlbytefwd-qci70
pgw-subdatastat-ulpktdrop-qci65
pgw-subdatastat-ulpktdrop-qci66

```

pgw-subdatastat-ulpktdrop-qci69
 pgw-subdatastat-ulpktdrop-qci70
 pgw-subdatastat-ulbytedrop-qci65
 pgw-subdatastat-ulbytedrop-qci66
 pgw-subdatastat-ulbytedrop-qci69
 pgw-subdatastat-ulbytedrop-qci70
 pgw-subdatastat-dlpktdrop-qci65
 pgw-subdatastat-dlpktdrop-qci66
 pgw-subdatastat-dlpktdrop-qci69
 pgw-subdatastat-dlpktdrop-qci70
 pgw-subdatastat-dlbytedrop-qci65
 pgw-subdatastat-dlbytedrop-qci66
 pgw-subdatastat-dlbytedrop-qci69
 pgw-subdatastat-dlbytedrop-qci70
 pgw-subdatastat-ulpktdropmbrexc-qci65
 pgw-subdatastat-ulpktdropmbrexc-qci66
 pgw-subdatastat-ulpktdropmbrexc-qci69
 pgw-subdatastat-ulpktdropmbrexc-qci70
 pgw-subdatastat-ulbytedropmbrexc-qci65
 pgw-subdatastat-ulbytedropmbrexc-qci66
 pgw-subdatastat-ulbytedropmbrexc-qci69
 pgw-subdatastat-ulbytedropmbrexc-qci70
 pgw-subdatastat-dlpktdropmbrexc-qci65
 pgw-subdatastat-dlpktdropmbrexc-qci66
 pgw-subdatastat-dlpktdropmbrexc-qci69
 pgw-subdatastat-dlpktdropmbrexc-qci70
 pgw-subdatastat-dlbytedropmbrexc-qci65
 pgw-subdatastat-dlbytedropmbrexc-qci66
 pgw-subdatastat-dlbytedropmbrexc-qci69
 pgw-subdatastat-dlbytedropmbrexc-qci70
 collapsed-subdatastat-ulpktfwd-qci65
 collapsed-subdatastat-ulpktfwd-qci66
 collapsed-subdatastat-ulpktfwd-qci69
 collapsed-subdatastat-ulpktfwd-qci70
 collapsed-subdatastat-ulbytefwd-qci65
 collapsed-subdatastat-ulbytefwd-qci66
 collapsed-subdatastat-ulbytefwd-qci69
 collapsed-subdatastat-ulbytefwd-qci70
 collapsed-subdatastat-dlpktfwd-qci65
 collapsed-subdatastat-dlpktfwd-qci66
 collapsed-subdatastat-dlpktfwd-qci69
 collapsed-subdatastat-dlpktfwd-qci70
 collapsed-subdatastat-dlbytefwd-qci65
 collapsed-subdatastat-dlbytefwd-qci66
 collapsed-subdatastat-dlbytefwd-qci69
 collapsed-subdatastat-dlbytefwd-qci70
 collapsed-subdatastat-ulpktdrop-qci65
 collapsed-subdatastat-ulpktdrop-qci66
 collapsed-subdatastat-ulpktdrop-qci69
 collapsed-subdatastat-ulpktdrop-qci70
 collapsed-subdatastat-ulbytedrop-qci65
 collapsed-subdatastat-ulbytedrop-qci66
 collapsed-subdatastat-ulbytedrop-qci69
 collapsed-subdatastat-ulbytedrop-qci70
 collapsed-subdatastat-dlpktdrop-qci65
 collapsed-subdatastat-dlpktdrop-qci66
 collapsed-subdatastat-dlpktdrop-qci69
 collapsed-subdatastat-dlpktdrop-qci70
 collapsed-subdatastat-dlbytedrop-qci65
 collapsed-subdatastat-dlbytedrop-qci66
 collapsed-subdatastat-dlbytedrop-qci69
 collapsed-subdatastat-dlbytedrop-qci70
 collapsed-subgosstat-bearact-qci65
 collapsed-subgosstat-bearact-qci66
 collapsed-subgosstat-bearact-qci69
 collapsed-subgosstat-bearact-qci70
 collapsed-subgosstat-bearset-qci65
 collapsed-subgosstat-bearset-qci66
 collapsed-subgosstat-bearset-qci69
 collapsed-subgosstat-bearset-qci70
 collapsed-subgosstat-bearrel-qci65
 collapsed-subgosstat-bearrel-qci66
 collapsed-subgosstat-bearrel-qci69

collapsed-subqosstat-bearrel-qci70
 saegw-ggsn-subqosstat-bearact-qci65
 saegw-ggsn-subqosstat-bearact-qci66
 saegw-ggsn-subqosstat-bearact-qci69
 saegw-ggsn-subqosstat-bearact-qci70
 saegw-ggsn-subqosstat-bearset-qci65
 saegw-ggsn-subqosstat-bearset-qci66
 saegw-ggsn-subqosstat-bearset-qci69
 saegw-ggsn-subqosstat-bearset-qci70
 saegw-ggsn-subqosstat-bearrel-qci65
 saegw-ggsn-subqosstat-bearrel-qci66
 saegw-ggsn-subqosstat-bearrel-qci69
 saegw-ggsn-subqosstat-bearrel-qci70
 saegw-ggsn-subdatastat-ulpktfwd-qci65
 saegw-ggsn-subdatastat-ulpktfwd-qci66
 saegw-ggsn-subdatastat-ulpktfwd-qci69
 saegw-ggsn-subdatastat-ulpktfwd-qci70
 saegw-ggsn-subdatastat-ulbytefwd-qci65
 saegw-ggsn-subdatastat-ulbytefwd-qci66
 saegw-ggsn-subdatastat-ulbytefwd-qci69
 saegw-ggsn-subdatastat-ulbytefwd-qci70
 saegw-ggsn-subdatastat-dlpktfwd-qci65
 saegw-ggsn-subdatastat-dlpktfwd-qci66
 saegw-ggsn-subdatastat-dlpktfwd-qci69
 saegw-ggsn-subdatastat-dlpktfwd-qci70
 saegw-ggsn-subdatastat-dlbytefwd-qci65
 saegw-ggsn-subdatastat-dlbytefwd-qci66
 saegw-ggsn-subdatastat-dlbytefwd-qci69
 saegw-ggsn-subdatastat-dlbytefwd-qci70
 saegw-ggsn-subdatastat-ulpktdrop-qci65
 saegw-ggsn-subdatastat-ulpktdrop-qci66
 saegw-ggsn-subdatastat-ulpktdrop-qci69
 saegw-ggsn-subdatastat-ulpktdrop-qci70
 saegw-ggsn-subdatastat-ulbytedrop-qci65
 saegw-ggsn-subdatastat-ulbytedrop-qci66
 saegw-ggsn-subdatastat-ulbytedrop-qci69
 saegw-ggsn-subdatastat-ulbytedrop-qci70
 saegw-ggsn-subdatastat-dlpktdrop-qci65
 saegw-ggsn-subdatastat-dlpktdrop-qci66
 saegw-ggsn-subdatastat-dlpktdrop-qci69
 saegw-ggsn-subdatastat-dlpktdrop-qci70
 saegw-ggsn-subdatastat-dlbytedrop-qci65
 saegw-ggsn-subdatastat-dlbytedrop-qci66
 saegw-ggsn-subdatastat-dlbytedrop-qci69
 saegw-ggsn-subdatastat-dlbytedrop-qci70
 saegw-ggsn-subdatastat-ulpktdropmbrexc-qci65
 saegw-ggsn-subdatastat-ulpktdropmbrexc-qci66
 saegw-ggsn-subdatastat-ulpktdropmbrexc-qci69
 saegw-ggsn-subdatastat-ulpktdropmbrexc-qci70
 saegw-ggsn-subdatastat-ulbytedropmbrexc-qci65
 saegw-ggsn-subdatastat-ulbytedropmbrexc-qci66
 saegw-ggsn-subdatastat-ulbytedropmbrexc-qci69
 saegw-ggsn-subdatastat-ulbytedropmbrexc-qci70
 saegw-ggsn-subdatastat-dlpktdropmbrexc-qci65
 saegw-ggsn-subdatastat-dlpktdropmbrexc-qci66
 saegw-ggsn-subdatastat-dlpktdropmbrexc-qci69
 saegw-ggsn-subdatastat-dlpktdropmbrexc-qci70
 saegw-ggsn-subdatastat-dlbytedropmbrexc-qci65
 saegw-ggsn-subdatastat-dlbytedropmbrexc-qci66
 saegw-ggsn-subdatastat-dlbytedropmbrexc-qci69
 saegw-ggsn-subdatastat-dlbytedropmbrexc-qci70

S-GW Schema

The following bulk statistics have been added to the S-GW schema to support the New Standard QCIs feature.

totepsbearactive-qci65
 totepsbearactive-qci66
 totepsbearactive-qci69
 totepsbearactive-qci70
 totepsbearsetup-qci65

```

totepsbearsetup-qci66
totepsbearsetup-qci69
totepsbearsetup-qci70
totepsbearrel-qci65
totepsbearrel-qci66
totepsbearrel-qci69
totepsbearrel-qci70
totepsbearmod-qci65
totepsbearmod-qci66
totepsbearmod-qci69
totepsbearmod-qci70
totepsbearrel-dedrsn-pgw-qci65
totepsbearrel-dedrsn-pgw-qci66
totepsbearrel-dedrsn-pgw-qci69
totepsbearrel-dedrsn-pgw-qci70
totepsbearrel-dedrsn-slerr-qci65
totepsbearrel-dedrsn-slerr-qci66
totepsbearrel-dedrsn-slerr-qci69
totepsbearrel-dedrsn-slerr-qci70
totepsbearrel-dedrsn-s5err-qci65
totepsbearrel-dedrsn-s5err-qci66
totepsbearrel-dedrsn-s5err-qci69
totepsbearrel-dedrsn-s5err-qci70
totepsbearrel-dedrsn-s4err-qci65
totepsbearrel-dedrsn-s4err-qci66
totepsbearrel-dedrsn-s4err-qci69
totepsbearrel-dedrsn-s4err-qci70
totepsbearrel-dedrsn-s12err-qci65
totepsbearrel-dedrsn-s12err-qci66
totepsbearrel-dedrsn-s12err-qci69
totepsbearrel-dedrsn-s12err-qci70
totepsbearrel-dedrsn-local-qci65
totepsbearrel-dedrsn-local-qci66
totepsbearrel-dedrsn-local-qci69
totepsbearrel-dedrsn-local-qci70
totepsbearrel-dedrsn-pdn-qci65
totepsbearrel-dedrsn-pdn-qci66
totepsbearrel-dedrsn-pdn-qci69
totepsbearrel-dedrsn-pdn-qci70
totepsbearrel-dedrsn-pathfail-s1-u-qci65
totepsbearrel-dedrsn-pathfail-s1-u-qci66
totepsbearrel-dedrsn-pathfail-s1-u-qci69
totepsbearrel-dedrsn-pathfail-s1-u-qci70
totepsbearrel-dedrsn-pathfail-s5-u-qci65
totepsbearrel-dedrsn-pathfail-s5-u-qci66
totepsbearrel-dedrsn-pathfail-s5-u-qci69
totepsbearrel-dedrsn-pathfail-s5-u-qci70
totepsbearrel-dedrsn-pathfail-s5-qci65
totepsbearrel-dedrsn-pathfail-s5-qci66
totepsbearrel-dedrsn-pathfail-s5-qci69
totepsbearrel-dedrsn-pathfail-s5-qci70
totepsbearrel-dedrsn-pathfail-s11-qci65
totepsbearrel-dedrsn-pathfail-s11-qci66
totepsbearrel-dedrsn-pathfail-s11-qci69
totepsbearrel-dedrsn-pathfail-s11-qci70
totepsbearrel-dedrsn-pathfail-s12-qci65
totepsbearrel-dedrsn-pathfail-s12-qci66
totepsbearrel-dedrsn-pathfail-s12-qci69
totepsbearrel-dedrsn-pathfail-s12-qci70
totepsbearrel-dedrsn-pathfail-s4-u-qci65
totepsbearrel-dedrsn-pathfail-s4-u-qci66
totepsbearrel-dedrsn-pathfail-s4-u-qci69
totepsbearrel-dedrsn-pathfail-s4-u-qci70
totepsbearrel-dedrsn-inactivity-timeout-qci65
totepsbearrel-dedrsn-inactivity-timeout-qci66
totepsbearrel-dedrsn-inactivity-timeout-qci69
totepsbearrel-dedrsn-inactivity-timeout-qci70
totepsbearrel-dedrsn-other-qci65
totepsbearrel-dedrsn-other-qci66
totepsbearrel-dedrsn-other-qci69
totepsbearrel-dedrsn-other-qci70
datastat-uplink-qci65totbyte
datastat-uplink-qci65totpkt

```

```

datastat-uplink-qci66totbyte
datastat-uplink-qci66totpkt
datastat-uplink-qci69totbyte
datastat-uplink-qci69totpkt
datastat-uplink-qci70totbyte
datastat-uplink-qci70totpkt
datastat-uplink-dropstat-qci65totbyte
datastat-uplink-dropstat-qci65totpkt
datastat-uplink-dropstat-qci66totbyte
datastat-uplink-dropstat-qci66totpkt
datastat-uplink-dropstat-qci69totbyte
datastat-uplink-dropstat-qci69totpkt
datastat-uplink-dropstat-qci70totbyte
datastat-uplink-dropstat-qci70totpkt
datastat-downlink-qci65totbyte
datastat-downlink-qci65totpkt
datastat-downlink-qci66totbyte
datastat-downlink-qci66totpkt
datastat-downlink-qci69totbyte
datastat-downlink-qci69totpkt
datastat-downlink-qci70totbyte
datastat-downlink-qci70totpkt
datastat-downlink-dropstat-qci65totbyte
datastat-downlink-dropstat-qci65totpkt
datastat-downlink-dropstat-qci66totbyte
datastat-downlink-dropstat-qci66totpkt
datastat-downlink-dropstat-qci69totbyte
datastat-downlink-dropstat-qci69totpkt
datastat-downlink-dropstat-qci70totbyte
datastat-downlink-dropstat-qci70totpkt
slu-uplnk-qci65totbyte
slu-uplnk-qci65totpkt
slu-uplnk-qci66totbyte
slu-uplnk-qci66totpkt
slu-uplnk-qci69totbyte
slu-uplnk-qci69totpkt
slu-uplnk-qci70totbyte
slu-uplnk-qci70totpkt
slu-uplnk-drop-qci65totbyte
slu-uplnk-drop-qci65totpkt
slu-uplnk-drop-qci66totbyte
slu-uplnk-drop-qci66totpkt
slu-uplnk-drop-qci69totbyte
slu-uplnk-drop-qci69totpkt
slu-uplnk-drop-qci70totbyte
slu-uplnk-drop-qci70totpkt
slu-downlnk-qci65totbyte
slu-downlnk-qci65totpkt
slu-downlnk-qci66totbyte
slu-downlnk-qci66totpkt
slu-downlnk-qci69totbyte
slu-downlnk-qci69totpkt
slu-downlnk-qci70totbyte
slu-downlnk-qci70totpkt
slu-downlnk-drop-qci65totbyte
slu-downlnk-drop-qci65totpkt
slu-downlnk-drop-qci66totbyte
slu-downlnk-drop-qci66totpkt
slu-downlnk-drop-qci69totbyte
slu-downlnk-drop-qci69totpkt
slu-downlnk-drop-qci70totbyte
slu-downlnk-drop-qci70totpkt
s4u-uplnk-qci65totbyte
s4u-uplnk-qci65totpkt
s4u-uplnk-qci66totbyte
s4u-uplnk-qci66totpkt
s4u-uplnk-qci69totbyte
s4u-uplnk-qci69totpkt
s4u-uplnk-qci70totbyte
s4u-uplnk-qci70totpkt
s4u-uplnk-drop-qci65totbyte
s4u-uplnk-drop-qci65totpkt
s4u-uplnk-drop-qci66totbyte

```

```

s4u-uplnk-drop-qci66totpkt
s4u-uplnk-drop-qci69totbyte
s4u-uplnk-drop-qci69totpkt
s4u-uplnk-drop-qci70totbyte
s4u-uplnk-drop-qci70totpkt
s4u-downlnk-qci65totbyte
s4u-downlnk-qci65totpkt
s4u-downlnk-qci66totbyte
s4u-downlnk-qci66totpkt
s4u-downlnk-qci69totbyte
s4u-downlnk-qci69totpkt
s4u-downlnk-qci70totbyte
s4u-downlnk-qci70totpkt
s4u-downlnk-drop-qci65totbyte
s4u-downlnk-drop-qci65totpkt
s4u-downlnk-drop-qci66totbyte
s4u-downlnk-drop-qci66totpkt
s4u-downlnk-drop-qci69totbyte
s4u-downlnk-drop-qci69totpkt
s4u-downlnk-drop-qci70totbyte
s4u-downlnk-drop-qci70totpkt
s12-uplnk-qci65totbyte
s12-uplnk-qci65totpkt
s12-uplnk-qci66totbyte
s12-uplnk-qci66totpkt
s12-uplnk-qci69totbyte
s12-uplnk-qci69totpkt
s12-uplnk-qci70totbyte
s12-uplnk-qci70totpkt
s12-uplnk-drop-qci65totbyte
s12-uplnk-drop-qci65totpkt
s12-uplnk-drop-qci66totbyte
s12-uplnk-drop-qci66totpkt
s12-uplnk-drop-qci69totbyte
s12-uplnk-drop-qci69totpkt
s12-uplnk-drop-qci70totbyte
s12-uplnk-drop-qci70totpkt
s12-downlnk-qci65totbyte
s12-downlnk-qci65totpkt
s12-downlnk-qci66totbyte
s12-downlnk-qci66totpkt
s12-downlnk-qci69totbyte
s12-downlnk-qci69totpkt
s12-downlnk-qci70totbyte
s12-downlnk-qci70totpkt
s12-downlnk-drop-qci65totbyte
s12-downlnk-drop-qci65totpkt
s12-downlnk-drop-qci66totbyte
s12-downlnk-drop-qci66totpkt
s12-downlnk-drop-qci69totbyte
s12-downlnk-drop-qci69totpkt
s12-downlnk-drop-qci70totbyte
s12-downlnk-drop-qci70totpkt
s5-uplnk-qci65totbyte
s5-uplnk-qci65totpkt
s5-uplnk-qci66totbyte
s5-uplnk-qci66totpkt
s5-uplnk-qci69totbyte
s5-uplnk-qci69totpkt
s5-uplnk-qci70totbyte
s5-uplnk-qci70totpkt
s5-uplnk-drop-qci65totbyte
s5-uplnk-drop-qci65totpkt
s5-uplnk-drop-qci66totbyte
s5-uplnk-drop-qci66totpkt
s5-uplnk-drop-qci69totbyte
s5-uplnk-drop-qci69totpkt
s5-uplnk-drop-qci70totbyte
s5-uplnk-drop-qci70totpkt
s5-downlnk-qci65totbyte
s5-downlnk-qci65totpkt
s5-downlnk-qci66totbyte
s5-downlnk-qci66totpkt

```

s5-downlnk-qci69totbyte
s5-downlnk-qci69totpkt
s5-downlnk-qci70totbyte
s5-downlnk-qci70totpkt
s5-downlnk-drop-qci65totbyte
s5-downlnk-drop-qci65totpkt
s5-downlnk-drop-qci66totbyte
s5-downlnk-drop-qci66totpkt
s5-downlnk-drop-qci69totbyte
s5-downlnk-drop-qci69totpkt
s5-downlnk-drop-qci70totbyte
s5-downlnk-drop-qci70totpkt
s8-uplnk-qci65totbyte
s8-uplnk-qci65totpkt
s8-uplnk-qci66totbyte
s8-uplnk-qci66totpkt
s8-uplnk-qci69totbyte
s8-uplnk-qci69totpkt
s8-uplnk-qci70totbyte
s8-uplnk-qci70totpkt
s8-uplnk-drop-qci65totbyte
s8-uplnk-drop-qci65totpkt
s8-uplnk-drop-qci66totbyte
s8-uplnk-drop-qci66totpkt
s8-uplnk-drop-qci69totbyte
s8-uplnk-drop-qci69totpkt
s8-uplnk-drop-qci70totbyte
s8-uplnk-drop-qci70totpkt
s8-downlnk-qci65totbyte
s8-downlnk-qci65totpkt
s8-downlnk-qci66totbyte
s8-downlnk-qci66totpkt
s8-downlnk-qci69totbyte
s8-downlnk-qci69totpkt
s8-downlnk-qci70totbyte
s8-downlnk-qci70totpkt
s8-downlnk-drop-qci65totbyte
s8-downlnk-drop-qci65totpkt
s8-downlnk-drop-qci66totbyte
s8-downlnk-drop-qci66totpkt
s8-downlnk-drop-qci69totbyte
s8-downlnk-drop-qci69totpkt
s8-downlnk-drop-qci70totbyte
s8-downlnk-drop-qci70totpkt
s5s8-uplnk-qci65totbyte
s5s8-uplnk-qci65totpkt
s5s8-uplnk-qci66totbyte
s5s8-uplnk-qci66totpkt
s5s8-uplnk-qci69totbyte
s5s8-uplnk-qci69totpkt
s5s8-uplnk-qci70totbyte
s5s8-uplnk-qci70totpkt
s5s8-uplnk-drop-qci65totbyte
s5s8-uplnk-drop-qci65totpkt
s5s8-uplnk-drop-qci66totbyte
s5s8-uplnk-drop-qci66totpkt
s5s8-uplnk-drop-qci69totbyte
s5s8-uplnk-drop-qci69totpkt
s5s8-uplnk-drop-qci70totbyte
s5s8-uplnk-drop-qci70totpkt
s5s8-downlnk-qci65totbyte
s5s8-downlnk-qci65totpkt
s5s8-downlnk-qci66totbyte
s5s8-downlnk-qci66totpkt
s5s8-downlnk-qci69totbyte
s5s8-downlnk-qci69totpkt
s5s8-downlnk-qci70totbyte
s5s8-downlnk-qci70totpkt
s5s8-downlnk-drop-qci65totbyte
s5s8-downlnk-drop-qci65totpkt
s5s8-downlnk-drop-qci66totbyte
s5s8-downlnk-drop-qci66totpkt
s5s8-downlnk-drop-qci69totbyte

```
s5s8-downlnk-drop-qci69totpkt
s5s8-downlnk-drop-qci70totbyte
s5s8-downlnk-drop-qci70totpkt
```

System Schema

The following bulk statistics have been added to the System Schema to support the New Standard QCIs feature.

```
sess-bearerdur-5sec-qci65
sess-bearerdur-10sec-qci65
sess-bearerdur-30sec-qci65
sess-bearerdur-1min-qci65
sess-bearerdur-2min-qci65
sess-bearerdur-5min-qci65
sess-bearerdur-15min-qci65
sess-bearerdur-30min-qci65
sess-bearerdur-1hr-qci65
sess-bearerdur-4hr-qci65
sess-bearerdur-12hr-qci65
sess-bearerdur-24hr-qci65
sess-bearerdur-over24hr-qci65
sess-bearerdur-2day-qci65
sess-bearerdur-4day-qci65
sess-bearerdur-5day-qci65
sess-bearerdur-5sec-qci66
sess-bearerdur-10sec-qci66
sess-bearerdur-30sec-qci66
sess-bearerdur-1min-qci66
sess-bearerdur-2min-qci66
sess-bearerdur-5min-qci66
sess-bearerdur-15min-qci66
sess-bearerdur-30min-qci66
sess-bearerdur-1hr-qci66
sess-bearerdur-4hr-qci66
sess-bearerdur-12hr-qci66
sess-bearerdur-24hr-qci66
sess-bearerdur-over24hr-qci66
sess-bearerdur-2day-qci66
sess-bearerdur-4day-qci66
sess-bearerdur-5day-qci66
sess-bearerdur-5sec-qci69
sess-bearerdur-10sec-qci69
sess-bearerdur-30sec-qci69
sess-bearerdur-1min-qci69
sess-bearerdur-2min-qci69
sess-bearerdur-5min-qci69
sess-bearerdur-15min-qci69
sess-bearerdur-30min-qci69
sess-bearerdur-1hr-qci69
sess-bearerdur-4hr-qci69
sess-bearerdur-12hr-qci69
sess-bearerdur-24hr-qci69
sess-bearerdur-over24hr-qci69
sess-bearerdur-2day-qci69
sess-bearerdur-4day-qci69
sess-bearerdur-5day-qci69
sess-bearerdur-5sec-qci70
sess-bearerdur-10sec-qci70
sess-bearerdur-30sec-qci70
sess-bearerdur-1min-qci70
sess-bearerdur-2min-qci70
sess-bearerdur-5min-qci70
sess-bearerdur-15min-qci70
sess-bearerdur-30min-qci70
sess-bearerdur-1hr-qci70
sess-bearerdur-4hr-qci70
sess-bearerdur-12hr-qci70
sess-bearerdur-24hr-qci70
sess-bearerdur-over24hr-qci70
sess-bearerdur-2day-qci70
```

```
sess-bearerdur-4day-qci70
sess-bearerdur-5day-qci70
```

Show Commands

This section describes the show commands available to monitor the New Standard QCIs feature.

show apn statistics all

The output of this command has been enhanced to show administrative disconnects and bearer statistics for the new standard QCIs 65, 66, 69, and 70. New statistics are highlighted in *italics*.

```
...
4G Bearers Released By Reasons:

Admin disconnect:  QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9
                  0      0      0      0      0      0      0      0      0
Admin disconnect:  QCI65  QCI66  QCI69  QCI70
                  0      0      0      0

...

QCI 65:
Bearer Active:           0
Bearer Released:         0
Bearer setup:             0
Bearer Rejected:         0

Uplink Bytes forwarded:  0
Uplink pkts forwarded:   0
Uplink Bytes dropped:    0
Uplink pkts dropped:     0
Uplink Bytes dropped(MBR Excd): 0
Uplink pkts dropped(MBR Excd): 0
Downlink Bytes forwarded: 0
Downlink pkts forwarded:  0
Downlink Bytes dropped:    0
Downlink pkts dropped:     0
Downlink Bytes dropped(MBR Excd): 0
Downlink pkts dropped(MBR Excd): 0

QCI 66:
Bearer Active:           0
Bearer Released:         0
Bearer setup:             0
Bearer Rejected:         0

Uplink Bytes forwarded:  0
Uplink pkts forwarded:   0
Uplink Bytes dropped:    0
Uplink pkts dropped:     0
Uplink Bytes dropped(MBR Excd): 0
Uplink pkts dropped(MBR Excd): 0
Downlink Bytes forwarded: 0
Downlink pkts forwarded:  0
Downlink Bytes dropped:    0
Downlink pkts dropped:     0
Downlink Bytes dropped(MBR Excd): 0
Downlink pkts dropped(MBR Excd): 0

QCI 69:
Bearer Active:           0
Bearer Released:         0
Bearer setup:             0
Bearer Rejected:         0

Uplink Bytes forwarded:  0
Uplink pkts forwarded:   0
Uplink Bytes dropped:    0
Uplink pkts dropped:     0
Uplink Bytes dropped(MBR Excd): 0
Uplink pkts dropped(MBR Excd): 0
Downlink Bytes forwarded: 0
Downlink pkts forwarded:  0
Downlink Bytes dropped:    0
Downlink pkts dropped:     0
Downlink Bytes dropped(MBR Excd): 0
Downlink pkts dropped(MBR Excd): 0

QCI 70:
Bearer Active:           0
Bearer Released:         0
Bearer setup:             0
Bearer Rejected:         0

Uplink Bytes forwarded:  0
Uplink pkts forwarded:   0
Uplink Bytes dropped:    0
Uplink pkts dropped:     0
Uplink Bytes dropped(MBR Excd): 0
Uplink pkts dropped(MBR Excd): 0
Downlink Bytes forwarded: 0
Downlink pkts forwarded:  0
Downlink Bytes dropped:    0
Downlink pkts dropped:     0
Downlink Bytes dropped(MBR Excd): 0
Downlink pkts dropped(MBR Excd): 0
0
...
```

show gtpu statistics

The output of this command has been enhanced to provide packet and byte information for QCI values 65, 66, 69, and 70. New statistics are in *italics*.

```
...
QCI 9:
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0

QCI 65:
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0

QCI 66:
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0

QCI 69:
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0

QCI 70:
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0

Non-Std QCI (Non-GBR):
  Uplink Packets:      0  Uplink Bytes:      0
  Downlink Packets:    0  Downlink Bytes:    0
  Packets Discarded:   0  Bytes Discarded:  0
...
```

show pgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information by QoS characteristics and IPv4v6 PDN Data statistics. New statistics are in *italics*.

```
Bearers By QoS characteristics:
Active:
  QCI 1:      0      Setup:
               QCI 1:      0
...
  QCI 65:      0      QCI 65:      0
  QCI 66:      0      QCI 66:      0
  QCI 69:      0      QCI 69:      0
  QCI 70:      0      QCI 70:      0
...

Released:
  QCI 1:      0
...
  QCI 65:      0
  QCI 66:      0
  QCI 69:      0
  QCI 70:      0
...

IPv4v6 PDN Data Statistics:
Uplink :
...
  Packets:
    QCI 1:      0
...
Downlink :
...
  Packets:
    QCI 1:      0
```


QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0

show saegw-service statistics all verbose

The output of this command has been enhanced to provide information related to the new standard QCIs. New statistics are in *italics>*.

```
...
Bearers By QoS characteristics:
  Active:
    QCI 1: 0
    ...
    QCI 9: 0
    QCI 65: 0
    QCI 66: 0
    QCI 69: 0
    QCI 70: 0
    Non-Std QCI: 0
  Released:
    QCI 1: 0
    ...
    QCI 9: 0
    QCI 65: 0
    QCI 66: 0
    QCI 69: 0
    QCI 70: 0
    Non-Std QCI: 0

...
    Std QCI(Non-GBR): 0
    Std QCI(GBR): 0

  Uplink :
    Packets:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Bytes:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Dropped Packets:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Dropped Bytes:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0

  Downlink :
    Packets:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Bytes:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Dropped Packets:
      QCI 1: 0\
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
      Non-Std QCI: 0
    Dropped Bytes:
      QCI 1: 0
      ...
      QCI 65: 0
      QCI 66: 0
      QCI 69: 0
      QCI 70: 0
```

```

Non-Std QCI: 0
Setup Guard Timer Expired: 0
Non-Std QCI: 0

```

show sgw-service statistics all verbose

The output of this command has been enhanced to provide new standard QCI information. New statistics are highlighted in *italics>*.

```

...
Bearers By QoS characteristics:
Active:
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  ...
Released:
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  ...
Dedicated Bearers Released By Reason:
PGW Ini: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
S1 Error Ind: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
S4 Error Ind: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
Local: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
Path Failure S1-U: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  ...
Setup:
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  ...
Modified:
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  ...
PCRF Ini: 0
  ...
S5 Error Ind: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
S12 Error Ind: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
PDN Down: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0
  QCI 69: 0
  QCI 70: 0
  Non-Std QCI: 0
  ...
Path Failure S5-U: 0
  QCI 1: 0
  ...
  QCI 65: 0
  QCI 66: 0

```

QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Path Failure S5:	0	Path Failure S11:	0
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Path Failure S4-U:	0	Path Failure S12:	0
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Inactivity Timeout:	0	Other:	0
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
...			
Data Statistics Per Interface:			
S1-U Total Data Statistics:			
Uplink :		Downlink :	
...			
Packets:		Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Bytes:		Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Packets:		Dropped Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Bytes:		Dropped Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
S4-U Total Data Statistics:			

Uplink :		Downlink :	
Total Pkts:	0	Total Pkts:	0
Total Bytes:	0	Total Bytes:	0
Dropped Pkts:	0	Dropped Pkts:	0
Dropped Bytes:	0	Dropped Bytes:	0
Packets:		Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Bytes:		Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Packets:		Dropped Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Bytes:		Dropped Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
S12 Total Data Statistics:			
Uplink :		Downlink :	
Total Pkts:	0	Total Pkts:	0
Total Bytes:	0	Total Bytes:	0
Dropped Pkts:	0	Dropped Pkts:	0
Dropped Bytes:	0	Dropped Bytes:	0
Packets:		Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Bytes:		Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Packets:		Dropped Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0

QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Bytes:		Dropped Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
S5-U Total Data Statistics:			
Uplink :		Downlink :	
Total Pkts:	0	Total Pkts:	0
Total Bytes:	0	Total Bytes:	0
Dropped Pkts:	0	Dropped Pkts:	0
Dropped Bytes:	0	Dropped Bytes:	0
Packets:		Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Bytes:		Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Packets:		Dropped Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Dropped Bytes:		Dropped Bytes:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
S8-U Total Data Statistics:			
Uplink :		Downlink :	
Total Pkts:	0	Total Pkts:	0
Total Bytes:	0	Total Bytes:	0
Dropped Pkts:	0	Dropped Pkts:	0
Dropped Bytes:	0	Dropped Bytes:	0
Packets:		Packets:	
QCI 1:	0	QCI 1:	0
...			
QCI 65:	0	QCI 65:	0
QCI 66:	0	QCI 66:	0
QCI 69:	0	QCI 69:	0
QCI 70:	0	QCI 70:	0
Non-Std QCI:	0	Non-Std QCI:	0
Bytes:		Bytes:	
QCI 1:	0	QCI 1:	0

...					
	QCI 65:	0	QCI 65:	0	
	QCI 66:	0	QCI 66:	0	0
	QCI 69:	0	QCI 69:	0	0
	QCI 70:	0	QCI 70:	0	0
	Non-Std QCI:	0	Non-Std QCI:	0	0
	Dropped Packets:		Dropped Packets:		
	QCI 1:	0	QCI 1:	0	0
...					
	QCI 65:	0	QCI 65:	0	
	QCI 66:	0	QCI 66:	0	0
	QCI 69:	0	QCI 69:	0	0
	QCI 70:	0	QCI 70:	0	0
	Non-Std QCI:	0	Non-Std QCI:	0	0
	Dropped Bytes:		Dropped Bytes:		
	QCI 1:	0	QCI 1:	0	0
...					
	QCI 65:	0	QCI 65:	0	
	QCI 66:	0	QCI 66:	0	0
	QCI 69:	0	QCI 69:	0	0
	QCI 70:	0	QCI 70:	0	0
	Non-Std QCI:	0	Non-Std QCI:	0	0

Non-standard QCI Support

This section describes the Non-standard QCI Support feature.

Feature Description

Usually, only standards-based QCI values of 1 through 9 are supported on GGSN/P-GW/SAEGW/S-GW/ePDG. A license, however, allows non-standard QCIs (128-254) to be used on P-GW/GGSN (not standalone GGSN).

Licensing

Use of non-standard QCIs require that a valid license key be installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128-254. QCI values 0 and 10 to 255 are defined as follows:

- 0: Reserved
- 10-127: Reserved
- 128-254: Operator-specific/Non-standard QCI
- 255: Reserved

Unique operator-specific QCIs (128-254) can be used to differentiate between various services/applications carriers provide to the end users in their network.

Limitations

- Non-standard QCIs can only be supported with S5/S8/S2a/S2b interfaces.
- The Gn interface is not supported.

Standards Compliance

- 3GPP Specification TS 23.203: Policy and charging control architecture
- 3GPP Specification TS 29.212: Policy and Charging Control over Gx reference point

Configuring Non-standard QCI Support

The **operator-defined-qci** command in the QCI-QoS Mapping Configuration Mode configures the non-standard QCIs in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF. Unique DSCP parameters (uplink and downlink) and GBR or Non-GBR can also be configured.

As non-standard QCIs are not supported in GGSN, **pre-rel8-qos-mapping** is used as a reference for mapping the non-standard QCI values to pre-rel8 QoS values during 3G calls or GnGp handovers.

Configuring Non-standard QCI Support in P-GW

Use the following command to configure non-standard QCI support in P-GW so that calls can be accepted when non-standard QCI values are received from UE or PCRF.

configure

qci-qos-mapping *name*

```

    operator-defined-qci num { gbr | non-gbr } [ { downlink | uplink } [ encaps-header { copy-inner
| copy-outer | dscp-marking dscp-marking-value } [ internal-qos priority priority ] | internal-qos priority
priority | user-datagram dscp-marking dscp-marking-value [ encaps-header { copy-inner | copy-outer |
dscp-marking dscp-marking-value } [ internal-qos priority priority ] ] | pre-rel8-qos-mapping num ]
    no operator-defined-qci num
end

```

Notes:

- This command is only visible if the license key supporting non-standard QCIs is installed. Contact your Cisco Account or Support representative for information on how to obtain a license.
- **operator-defined-qci** *num*: Specifies the operator-defined QCI value to be enabled.
num must be an integer from 128 through 254.
Standards-based QCI values 1 through 9 are configured through the **qci** command.
- **pre-rel8-qos-mapping** *num*: Maps non-standard QCI to a standard QCI that has the characteristics (TC, THP, SI, TD, SSD) similar to desired pre-rel8 standard QoS values during 3G call or GnGp handover.
num must be an integer from 1 through 4 for GBR and 5 through 9 for non-GBR. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

3G GGSN Call

If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI under P-GW which is associated with a GGSN, then the 3G call would be rejected.

GnGp Handoff

- 1 If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for default bearer, then the handoff would be rejected.
- 2 If the **pre-rel8-qos-mapping** field is not configured for the non-standard QCI for dedicated bearer, then only that bearer would be rejected during handoff.
- 3 In the following scenario:
 - default bearer with standard QCI or non-standard QCI (with **pre-rel8-qos-mapping** configured)
 - more than one dedicated bearer (some with standard QCI, some with non-standard QCI with **pre-rel8-qos-mapping** configured, and some with non-standard QCI with no mapping)

During LTE-to-GnGp handoff:

- UPC Request for all the dedicated bearers with non-standard QCI with no mapping would be rejected
- handoff will be successful for the remaining bearers

Monitoring Non-standard QCI Support

Bulk Statistics

This section provides information regarding bulk statistics in support of non-standard QCI support.

APN Schema

The following counters have been added in support of non-standard QCIs (GBR and Non-GBR):

- nonstdqci-nongbr-uplinkpkt-drop-mbrexcd
- nonstdqci-nongbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-nongbr-uplinkbyte-drop-mbrexcd
- nonstdqci-nongbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-nongbr-rejbearer
- nonstdqci-gbr-uplinkpkt-drop-mbrexcd
- nonstdqci-gbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-gbr-uplinkbyte-drop-mbrexcd
- nonstdqci-gbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-gbr-rejbearer

Output of Show Commands

This section provides information regarding show commands and/or their outputs in support of non-standard QCI support.

show apn statistics

The output of this command has been enhanced to show the following non-standard QCI counters (GBR and Non-GBR):

- Non-Std QCI(Non-GBR)
 - Bearer Rejected
 - Uplink Bytes dropped(MBR Excd)
 - Downlink Bytes dropped(MBR Excd)
 - Uplink pkts dropped(MBR Excd)
 - Downlink pkts dropped(MBR Excd)
- Non-Std QCI(GBR)
 - Bearer Rejected
 - Uplink Bytes dropped(MBR Excd)
 - Downlink Bytes dropped(MBR Excd)
 - Uplink pkts dropped(MBR Excd)
 - Downlink pkts dropped(MBR Excd)

show qci-qos-mapping table all

The output of this command has been enhanced to show when non-standard QCI are configured:

- Operator-defined-qci
- pre-rel8-qos-mapping



GGSN UPC Collision Handling

- [GGSN UPC Collision Handling, page 343](#)

GGSN UPC Collision Handling

Feature Description

In StarOS 14.0 and earlier, during collision between SGSN initiated UPC request and GGSN Initiated UPC request, pre-defined rules were activated at GGSN without waiting for network requested UPC (NRUPC) response and there were no packet drops.

From StarOS release 15.0 onward, predefined rules were activated only on receiving NRUPC response at GGSN and not in case of collision. This resulted in packet drops.

In StarOS 20.0, the **GGSN UPC Collision Handling** feature addresses the problem of packet drops. During collision between SGSN initiated UPC request and GGSN initiated UPC Request, SGSN initiated UPC request gets higher priority over NRUPC and there is no call or data loss during call establishment or during mid-call phase. This feature can be enabled or disabled using a CLI and is enabled by default.

How It Works

In StarOS release 14.0 and earlier:

- Predefined rules were activated at GGSN without waiting for network requested UPC (NRUPC) response.
- SGSN initiated UPCReq was received at GGSN before NRUPC response (collision).
- SGSN initiated UPCReq aborted the NRUPC.
- Session manager (SM) did not send failure message to ECS.
- However, the predefined rules were already activated at GGSN (without waiting for NRUPC response). Hence, there were no packet drops.

From StarOS release 15.0 onward, predefined rules were activated only on receiving NRUPC response at GGSN and were not activated in case of collision. There was no static catch-all rule defined in rulebase. This caused packet drops.

In StarOS 20.0, the **GGSN UPC Collision Handling** feature addresses the problem of packet drops. During collision between SGSN initiated UPC request and GGSN initiated UPC Request, SGSN initiated UPC request gets higher priority over NRUPC and there is no call or data loss during call establishment or during mid-call phase. This feature can be enabled or disabled using a CLI and is enabled by default.

- When GGSN detects collision between SGSN initiated UPC request and NRUPC on primary PDP context, NRUPC is retried (with different sequence number) after sending UPC Response.
- When GGSN detects collision between SGSN initiated UPC request for Inter-SGSN handoff and NRUPC with TFT and after handoff BCM mode is changed from Mixed mode to MS-Only mode, NRUPC is retried (with different sequence number) after sending UPC Response, but without TFT.
- When GGSN detects collision between an SGSN initiated UPC and a NRUPC on secondary PDP context, NRUPC is aborted and PCRF is notified. When multiple CCR-U support is not enabled on GGSN, CCR-U for aborted NRUPC (on secondary PDP context) is not informed to PCRF. In this case, PCRF will not be aware of this aborted transaction (rule failure).

Limitations

- Behavior for GnGp GGSN has been modified for this feature, in this release. Behavior for GGSN remains unaltered.
- When NRUPC received from Direct Tunnel (due to "Direct Tunnel Error Indication") collides with SGSN initiated UPC request, NRUPC is aborted and not retried. This does not affect the functionality as, when "Direct Tunnel Error Indication" is received from access side, NRUPC is triggered again.
- When a request for handoff to LTE is received before receiving NRUPC response, the behavior remains unchanged. In this case, the pending NRUPC request is aborted. If the NRUPC request received is for rule installation, the request remains in the pending state and the rule is not installed. As there is no static rule and the rule installation request is in pending state, the PDP context stays up without an installed rule.

Configuring GGSN UPC Collision Handling

Operators can use the Command Line Interface (CLI) to configure the collision between SGSN initiated UPC request and network initiated UPC Request.

gtpc handle-collision

This command in the service configuration mode can be used to the collision between SGSN initiated UPC request and network initiated UPC Request.

GGSN Service

configure

context *context_name*

ggsn-service *service_name*

```
[ no | default | gtpc handle-collision upc nrupc
end
```

P-GW Service

configure

```
context context_name
pgw-service service_name
[ no | default | gtpc handle-collision upc nrupc
end
```

S-GW Service

configure

```
context context_name
sgw-service service_name
[ no | default | gtpc handle-collision upc nrupc
end
```

SAEGW Service

configure

```
context context_name
saegw-service service_name
[ no | default | gtpc handle-collision upc nrupc
end
```

Notes:

- **no:** Disables collision handling between SGSN initiated UPC and NRUPC request.
- **default:** Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.
- **handle-collision upc nrupc:** Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show configuration verbose**

Please see the *Monitoring and Troubleshooting GGSN UPC Collision Handling* section for the command output.

Monitoring and Troubleshooting GGSN UPC Collision Handling

The following section describes commands available to monitor GGSN UPC Collision Handling.

Show Commands for GGSN UPC Collision Handling

show configuration

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show configuration verbose

This command displays the following output:

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show ggsn-service name *service_name*

This command displays the following output:

```
Service name:                ggsn-service
Context:                    ingress
...
Suppress NRUPC triggered by UPC: Disabled
Collision handling for UPC-NRUPC: Enabled/Disabled
```

show gtpc statistics

This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:                1
  2G:                   0
  3G:                   1
...
...
MS Info Change Reporting Messages:
  MS Info Chng Notif Req: 0   Accepted:                0
  Denied:                 0   Discarded:                0

NRUPC UPC Collision:
  Primary PDP ctxt:      3   Secondary PDP ctxt:      0

QoS negotiation:
  CPC QoS Accepted:      3   CPC QoS Downgraded:      0
```

```
UPC QoS Accepted:          3    UPC QoS Downgraded:          0
```

show gtpc statistics [format1 | ggsn-service *service_name* | verbose]

This command displays the number of NRUPC and SGSN initiated UPC collisions happening for primary and secondary PDP context for a GGSN service. This command displays the following output:

```
Active Subscribers:
  Total:          1
  2G:             0
  3G:             1
...
...
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:  0    Accepted:          0
  Denied:                  0    Discarded:          0

NRUPC UPC Collision:
  Primary PDP ctxt:        3    Secondary PDP ctxt:    0

QoS negotiation:
  CPC QoS Accepted:        3    CPC QoS Downgraded:    0
  UPC QoS Accepted:        3    UPC QoS Downgraded:    0
```




GRE Protocol Interface

This chapter provides information on Generic Routing Encapsulation protocol interface support in the GGSN or P-GW service node. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

GRE protocol interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.



Important

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

- [Introduction, page 350](#)
- [Supported Standards, page 351](#)
- [Supported Networks and Platforms, page 351](#)
- [Licenses, page 351](#)
- [Services and Application on GRE Interface, page 351](#)
- [How GRE Interface Support Works, page 351](#)
- [GRE Interface Configuration, page 355](#)
- [Verifying Your Configuration, page 359](#)

Introduction

GRE protocol functionality adds one additional protocol on Cisco's multimedia core platforms (ASR 5500 or higher) to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiator.

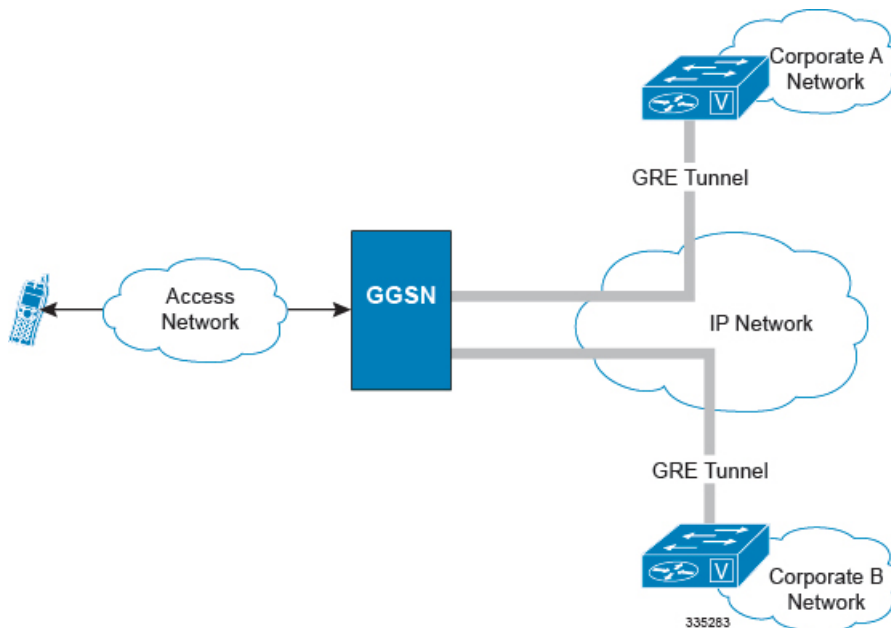
It is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSec.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

Figure 55: GRE Interface Deployment Scenario



Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 1701, Generic Routing Encapsulation (GRE)
- RFC 1702, Generic Routing Encapsulation over IPv4 networks
- RFC 2784, Generic Routing Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE

Supported Networks and Platforms

This feature supports all systems with StarOS Release 9.0 or later running GGSN and/or SGSN service for the core network services. The P-GW service supports this feature with StarOS Release 12.0 or later.

Licenses

GRE protocol interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Services and Application on GRE Interface

GRE interface implementation provides the following functionality with GRE protocol support.

How GRE Interface Support Works

The GRE interface provides two types of data processing; one for ingress packets and another for egress packets.

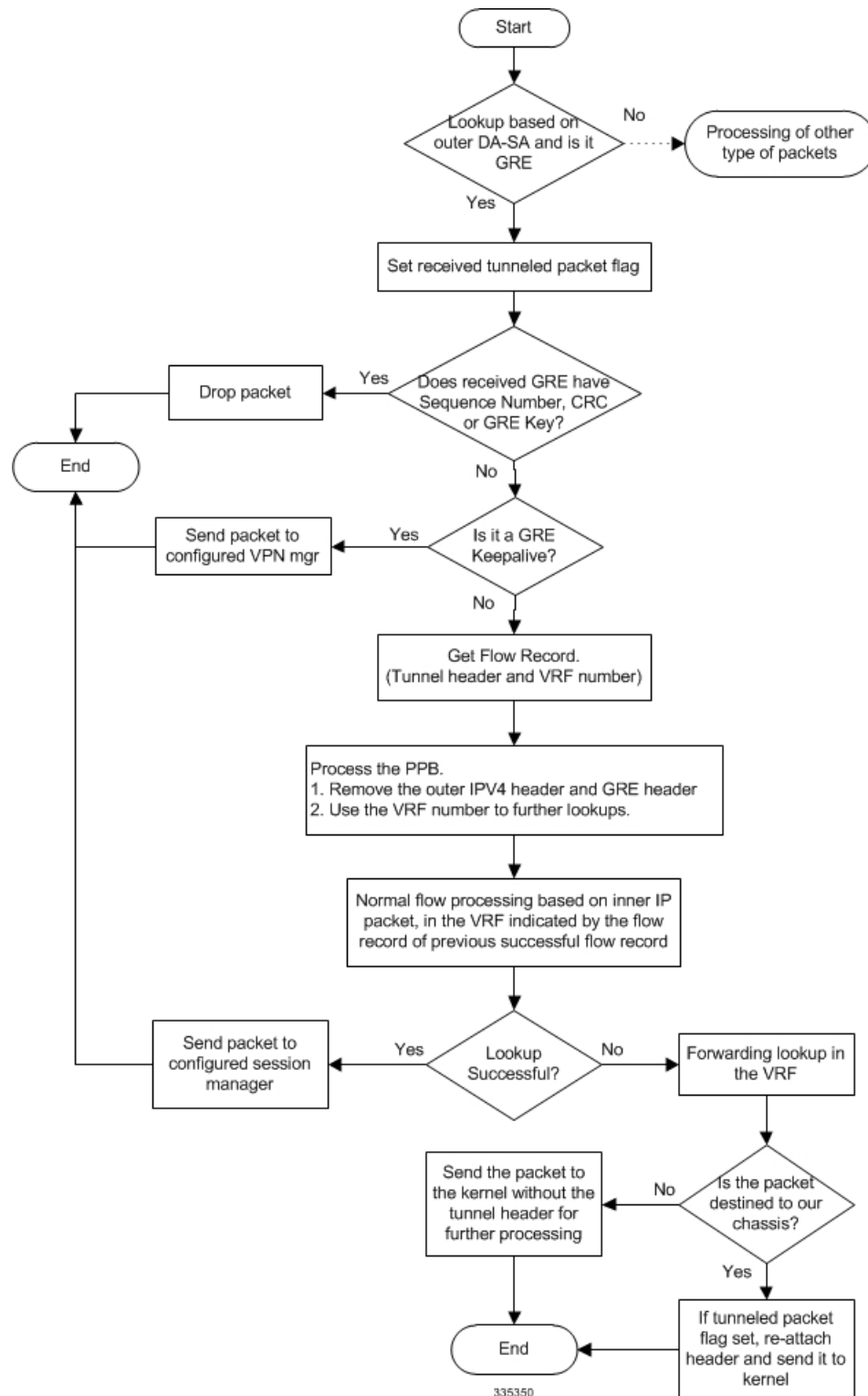
Ingress Packet Processing on GRE Interface

Figure given below provides a flow of process for incoming packets on GRE interface.

Note that in case the received packet is a GRE keep-alive or a ping packet then the outer IPV4 and GRE header are not stripped off (or get reattached), but instead the packet is forwarded as is to the VPN manager or kernel

respectively. In case of all other GRE tunneled packets the IPV4 and GRE header are stripped off before sending the packet for a new flow lookup.

Figure 56: Ingress Packet Processing on GRE Interface

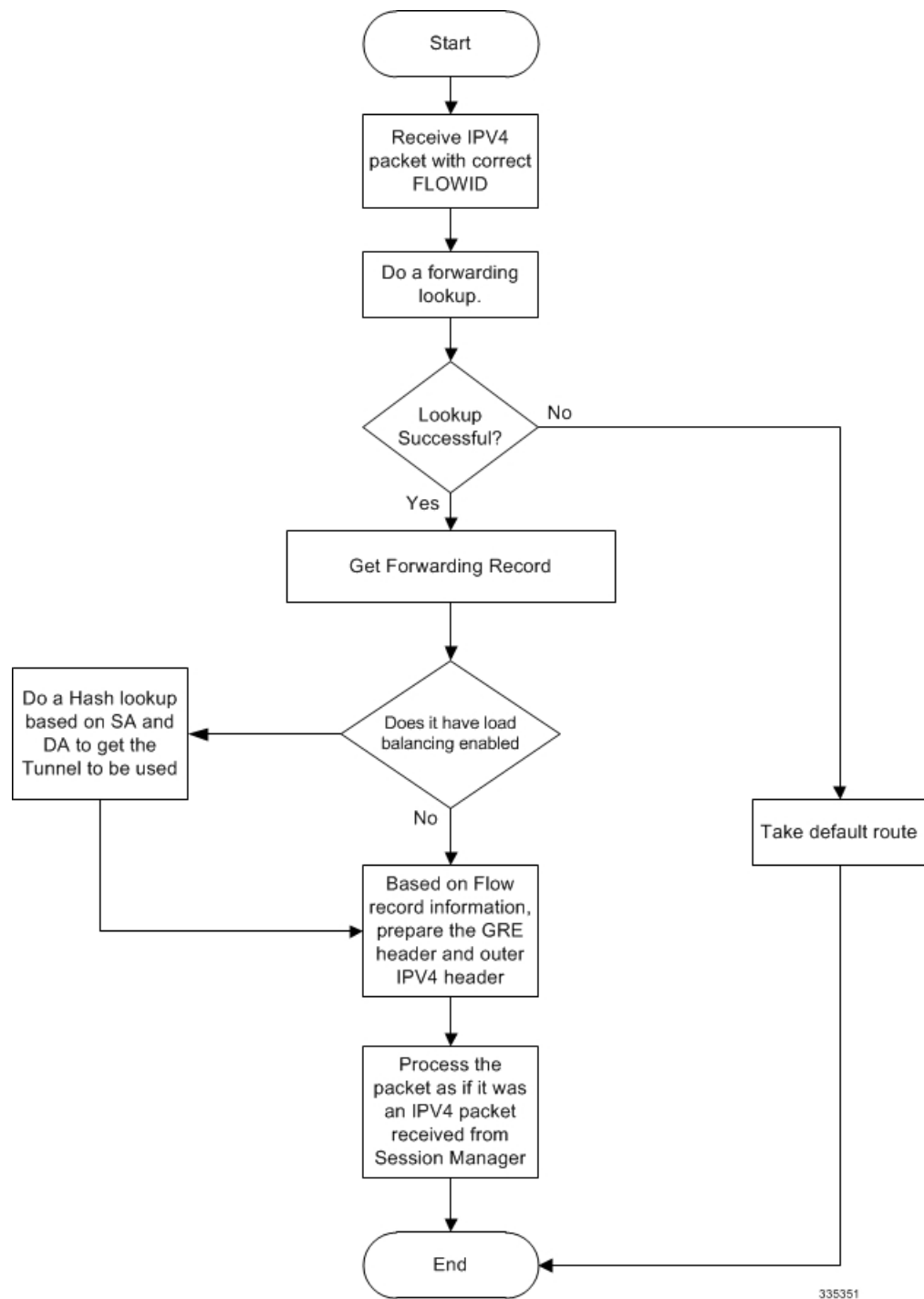


3353350

Egress Packet Processing on GRE Interface

Figure given below provides a flow of process for outgoing packets on GRE interface:

Figure 57: Egress Packet Processing on GRE Interface



335351

GRE Interface Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with GRE interface in GGSN or P-GW services.

**Important**

This section provides the minimum instruction set to enable the GRE Protocol Interface support functionality on a GGSN or P-GW. Commands that configure additional functions for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and specific product Administration Guide.

To configure the system to support GRE tunnel interface:

-
- Step 1** Configure the virtual routing and forwarding (VRF) in a context by applying the example configurations presented in [Virtual Routing And Forwarding \(VRF\) Configuration, on page 356](#).
 - Step 2** Configure the GRE tunnel interface in a context by applying the example configurations presented in [GRE Tunnel Interface Configuration, on page 357](#).
 - Step 3** Enable OSPF for the VRF and for the given network by applying the example configurations presented in [Enabling OSPF for VRF, on page 357](#).
 - Step 4** Associate IP pool and AAA server group with VRF by applying the example configurations presented in [Associating IP Pool and AAA Group with VRF, on page 358](#).
 - Step 5** Associate APN with VRF through AAA server group and IP pool by applying the example configurations presented in [Associating APN with VRF, on page 358](#).
 - Step 6** Optional. If the route to the server is not learnt from the corporate over OSPFv2, static route can be configured by applying the example configurations presented in [Static Route Configuration, on page 359](#).
 - Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
 - Step 8** Verify configuration of GRE and VRF related parameters by applying the commands provided in [Verifying Your Configuration, on page 359](#).
-

Virtual Routing And Forwarding (VRF) Configuration

This section provides the configuration example to configure the VRF in a context:

```
configure
context <vpn_context_name> -noconfirm ]
    ip vrf <vrf_name>
        ip maximum-routes <max_routes>
    end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for VRF. For more information, refer *System Administration Guide*.
- A maximum of 300 VRFs per context and up to 2,048 VRFs per chassis can be configured on system.
- <vrf_name> is name of the VRF which is to be associated with various interfaces.
- A maximum of 10000 routes can be configured through **ip maximum-routes <max_routes>** command.

GRE Tunnel Interface Configuration

This section provides the configuration example to configure the GRE tunnel interface and associate a VRF with GRE interface:

```
configure
context <vpn_context_name>
  ip interface <intfc_name> tunnel
    ip vrf forwarding <vrf_name>
    ip address <internal_ip_address/mask>
    tunnel-mode gre
    source interface <non_tunn_intfc_to_corp>
    destination address <global_ip_address>
    keepalive interval <value> num-retry <retry>
  end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for GRE interface configuration. For more information, refer *Command Line Interface Reference*.
- A maximum of 511 GRE tunnels + 1 non-tunnel interface can be configured in one context. System needs at least 1 non-tunnel interface as a default.
- <intfc_name> is name of the IP interface which is defined as a tunnel type interface and to be used for GRE tunnel interface.
- <vrf_name> is the name of the VRF which is preconfigured in context configuration mode.
- <internal_ip_address/mask> is the network IP address with sub-net mask to be used for VRF forwarding.
- <non_tunn_intfc_to_corp> is the name a non-tunnel interface which is required by system as source interface and preconfigured. For more information on interface configuration refer *System Administration Guide*.
- <global_ip_address> is a globally reachable IP address to be used as a destination address.

Enabling OSPF for VRF

This section provides the configuration example to enable the OSPF for VRF to support GRE tunnel interface:

```
configure
context <vpn_context_name>
  router ospf
    ip vrf <vrf_name>
    network <internal_ip_address/mask>
  end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for OSPF routing. For more information, refer *Routing* in this guide.
- <vrf_name> is the name of the VRF which is preconfigured in context configuration mode.
- <internal_ip_address/mask> is the network IP address with sub-net mask to be used for OSPF routing.

Associating IP Pool and AAA Group with VRF

This section provides the configuration example for associating IP pool and AAA groups with VRF:

```
configure
context <vpn_context_name>
  ip pool <ip_pool_name> <internal_ip_address/mask> vrf <vrf_name>
  exit
  aaa group <aaa_server_group>
  ip vrf <vrf_name>
end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for IP pool and AAA server group.
- <ip_pool_name> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <aaa_server_group> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <vrf_name> is the name of the VRF which is preconfigured in context configuration mode.
- <internal_ip_address/mask> is the network IP address with sub-net mask to be used for IP pool.

Associating APN with VRF

This section provides the configuration example for associating an APN with VRF through AAA group and IP pool:

```
configure
context <vpn_context_name>
  apn <apn_name>
  aaa group <aaa_server_group>
  ip address pool name <ip_pool_name>
end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for APN configuration.
- <ip_pool_name> is name of a preconfigured IP pool. For more information refer *System Administration Guide*.
- <aaa_server_group> is name of a preconfigured AAA server group. For more information refer *AAA Interface Administration and Reference*.
- <vrf_name> is the name of the VRF which is preconfigured in context configuration mode.

Static Route Configuration

This section provides the optional configuration example for configuring static routes when the route to the server is not learnt from the corporate over OSPFv2:

```
configure
context <vpn_context_name>
  ip route <internal_ip_address/mask> tunnel <tunnel_intf_name> vrf <vrf_name>
end
```

Notes:

- <vpn_context_name> is the name of the system context you want to use for static route configuration.
- <internal_ip_address/mask> is the network IP address with sub-net mask to be used as static route.
- <tunnel_intf_name> is name of a predefined tunnel type IP interface which is to be used for GRE tunnel interface.
- <vrf_name> is the name of the VRF which is preconfigured in context configuration mode.

Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the *System Administration Guide* and also to retrieve errors and warnings within an active configuration for a service.



Important

All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the GRE interface configuration.

Step 1

Verify that your interfaces are configured properly by entering the following command in Exec Mode:

show ip interface

The output of this command displays the configuration of the all interfaces configured in a context.

```
Intf Name:      foo1
Intf Type:      Broadcast
Description:
IP State:       UP (Bound to 17/2 untagged, ifIndex 285343745)
IP Address:     1.1.1.1          Subnet Mask:      255.255.255.0
Bcast Address:  1.1.1.255       MTU:            1500
Resoln Type:    ARP            ARP timeout:     60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
Intf Name:      foo2
Intf Type:      Tunnel (GRE)
Description:
VRF:            vrf-tun
IP State:       UP (Bound to local address 1.1.1.1 (foo1), remote address 5.5.5.5)
IP Address:     10.1.1.1        Subnet Mask:      255.255.255.0
Intf Name:      foo3
Intf Type:      Tunnel (GRE)
Description:
```

```
IP State:          DOWN (<state explaining the reason of being down>)  
IP Address:        20.20.20.1          Subnet Mask:      255.255.255.0
```

Step 2

Verify that GRE keep alive is configured properly by entering the following command in Exec Mode:

show ip interface gre-keepalive

The output of this command displays the configuration of the keepalive for GRE interface configured in a context.



Gx Interface Support

This chapter provides information on configuring Gx interface to support policy and charging control for subscribers.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

The following topics are covered in this chapter:

- [Rel. 7 Gx Interface, page 361](#)
- [Rel. 8 Gx Interface, page 388](#)
- [Rel. 9 Gx Interface, page 411](#)
- [Rel. 10 Gx Interface, page 419](#)
- [Supported Gx Features, page 427](#)

Rel. 7 Gx Interface

Rel. 7 Gx interface support is available on the Cisco ASR chassis running StarOS 8.1 or StarOS 9.0 and later releases for the following products:

- GGSN
- IPSG

This section describes the following topics:

- [Introduction, on page 362](#)
- [Terminology and Definitions, on page 365](#)
- [How Rel. 7 Gx Works, on page 379](#)

- [Configuring Rel. 7 Gx Interface, on page 382](#)
- [Gathering Statistics, on page 387](#)

Introduction

For IMS deployment in GPRS/UMTS networks the system uses Rel. 7 Gx interface for policy-based admission control support and flow-based charging. The Rel. 7 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports flow-based charging. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and do charging. Other parameters associated with the rules are used to enforce policy control.

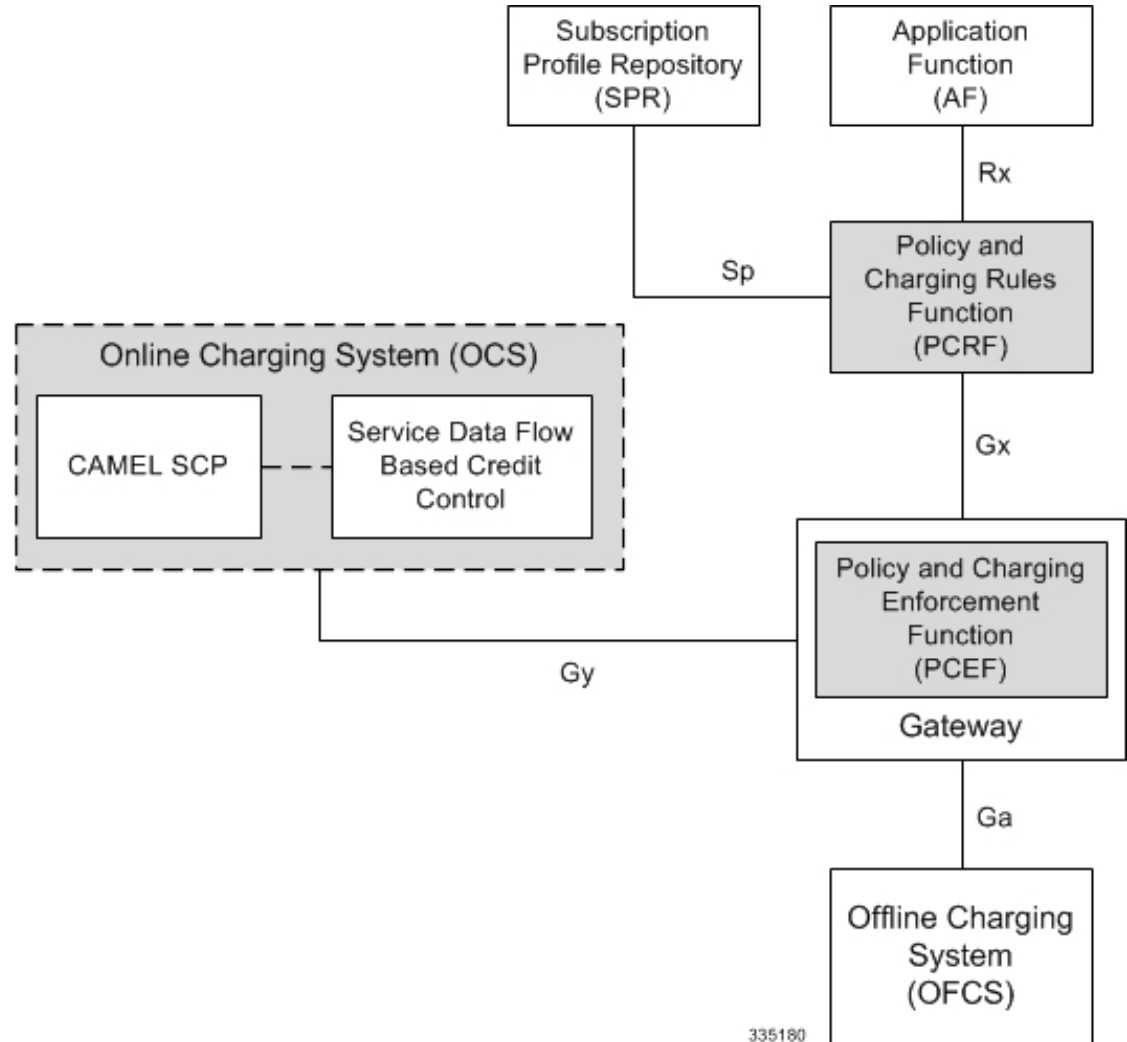
The PCC architecture allows operators to perform service-based QoS policy, and flow-based charging control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/Cisco Systems GGSN and the Policy and Charging Rules Function (PCRF).

In GPRS/UMTS networks, the client functionality lies with the GGSN, therefore in the IMS authorization scenario it is also called the Gateway. In the following figure, Gateway is the Cisco Systems GGSN, and the PCEF function is provided by Enhanced Charging Service (ECS). The Rel 7. Gx interface is implemented as a Diameter connection. The Gx messages mostly involve installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Rel. 7 Gx reference point is located between the Gateway and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway, and the transmission of traffic plane events from the Gateway to the PCRF. The Gx reference point can be used for charging control, policy control,

or both by applying AVPs relevant to the application. The following figure shows the reference points between various elements involved in the policy and charging architecture.

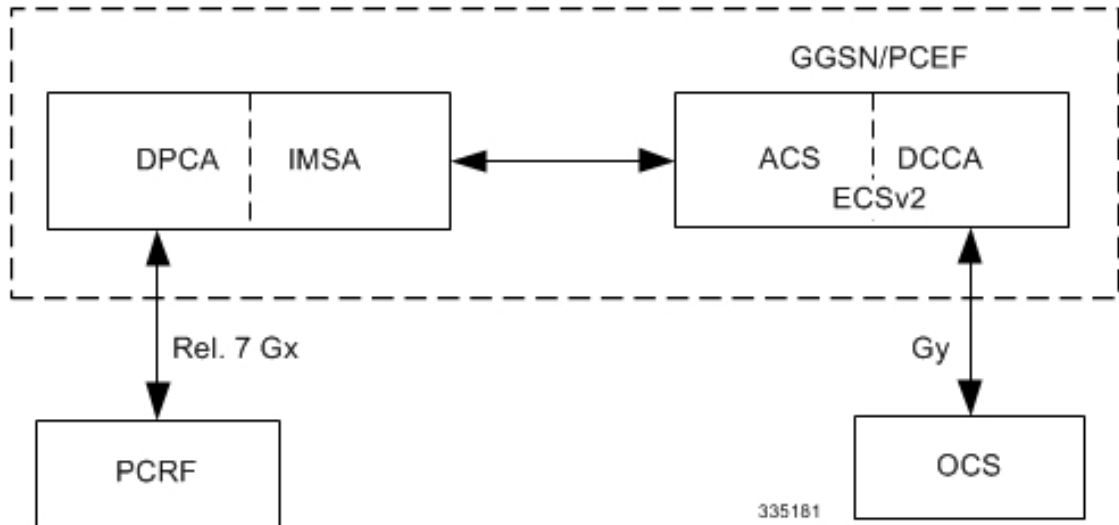
Figure 58: PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled

within the DCCA module (at the ECS). The following figure shows the interaction between components within the Gateway.

Figure 59: PCC Architecture within Cisco PCEF



Supported Networks and Platforms

This feature is supported on all chassis with StarOS Release 8.1 and later running GGSN service for the core network services.

License Requirements

The Rel. 7 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Supported Standards

The Rel 7. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.212 V7.8.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 7 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN bearer.

Policy control comprises the following functions:

- **Binding:** Binding is the generation of an association between a Service Data Flow (SDF) and the IP-CAN bearer (for GPRS a PDP context) transporting that SDF.

The QoS demand in the PCC rule, as well as the SDF template are input for the bearer binding. The selected bearer will have the same QoS Class as the one indicated by the PCC rule.

Depending on the type of IP-CAN and bearer control mode, bearer binding can be executed either by the PCRF, or both PCRF and PCEF.

- For UE-only IP-CAN bearer establishment mode, the PCRF performs bearer binding. When the PCRF performs bearer binding, it indicates the bearer (PDP context) by means of Bearer ID. The Bearer ID uniquely identifies the bearer within the PDP session.
- For UE/NW IP-CAN bearer establishment mode, the PCRF performs the binding of the PCC rules for user controlled services, while the PCEF performs the binding of the PCC rules for the network-controlled services.

Prior to Release 16.0, the rule binding was getting rejected. In 16.0 and later releases, the binding of PCEF rules will be successful when BCM mode is set to UE-only for EPS IP-CAN bearer without "bearer-ID" in the PCRF messages such as RAR or CCA-U.

In the 3G to 4G handover scenario, rule binding and rule removal will be successful in UE-only mode and any filter (and related info) changes because of this modification/installation/removal will not be notified to UE as updates in UE only mode cannot be sent to UE. These rules are only considered for charging and the expectation is that the same rules are again modified in 4G (if handover is done) so that the filters (and related info) can be notified to UE.

In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-U's to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- **Gating Control:** Gating control is the blocking or allowing of packets, belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is opened, the packets of the related IP flows are allowed to be forwarded.
- **Event Reporting:** Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF).

- Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level.

Note that in 11.0 and later releases, RAR with unknown event triggers are silently ignored and responded with DIAMETER_SUCCESS. In earlier releases, when unknown event triggers were received in the RAR command from PCRF, invalid AVP result code was set in the RAA command.

- The Event Reporting Function (ERF) receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response back to the PCRF. The Event Reporting Function is located in the PCEF.

In StarOS releases prior to 14.0, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger was sent for rules irrespective of successful installation. In 14.0 and later releases, SUCCESSFUL_RESOURCE_ALLOCATION (22) event trigger will be sent under the following conditions:

- When a rule is installed successfully (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).
- On partial failure, i.e., when two or more rules are installed and at least one of the rules were successfully installed. (and the event trigger is armed by PCRF and resource-allocation-notification is enabled).

On complete failure, i.e., none of the rules were installed, the event-trigger SUCCESSFUL_RESOURCE_ALLOCATION (22) will not be sent.



Important

In this release, event triggers "IP-CAN_CHANGE" and "MAX_NR_BEARERS_REACHED" are not supported.

- **QoS Control:** QoS control is the authorization and enforcement of the maximum QoS that is authorized for a SDF or an IP-CAN bearer or a QoS Class Identifier (QCI). In case of an aggregation of multiple SDFs (for GPRS a PDP context), the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate.
 - QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.
 - The enforcement of the authorized QoS of the IP-CAN bearer may lead to a downgrading or upgrading of the requested bearer QoS by the Gateway (PCEF) as part of a UE-initiated IP-CAN bearer establishment or modification. Alternatively, the enforcement of the authorized QoS may, depending on operator policy and network capabilities, lead to network-initiated IP-CAN bearer establishment or modification. If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.
 - QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. In case the PCRF provides PCC rules dynamically, authorized QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information

received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

**Important**

In this release, QoS Resource Reservation is not supported.

Supported Features:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Provisioning of "Authorized QoS" Per IP CAN Bearer: The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF.
- Policy Enforcement for "Authorized QoS" per IP CAN Bearer: The PCEF is responsible for enforcing the policy-based authorization, that is to ensure that the requested QoS is in-line with the "Authorized QoS" per IP CAN Bearer.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
 - Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
 - Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule. If the PCRF provides authorized QoS for both the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules takes place first.

**Important**

In this release, coordination of authorized QoS scopes in mixed mode (BCM = UE_NW) is not supported.

- ◦ Provisioning of Authorized QoS Per QCI: If the PCEF performs the bearer binding, the PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. If the PCRF performs the bearer binding the PCRF does not provision an authorized QoS per QCI. The PCRF does not provision an authorized QoS per QCI for GBR bearer QCI values.

**Important**

Only standards-based QCI values of 1 through 9 are supported. QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

- ◦ Policy Enforcement for Authorized QoS per QCI: The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values.

- Other Features:

- Bearer Control Mode Selection: The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session modification (as a consequence of an SGSN change). It will be done using the "PCC Rule Request" procedure.

If the Bearer-Control-Mode AVP is not received from PCRF, the IP-CAN session is not terminated. The value negotiated between UE/SGSN/GGSN is considered as the BCM. The following values are considered for each of the service types:

- GGSN: The negotiated value between UE/SGSN/GGSN is considered.

In the following scenarios UE_ONLY is chosen as the BCM:

Scenario 1:

- UE-> UE_ONLY
- SGSN-> UE_ONLY
- GGSN-> UE_ONLY
- PCRF-> NO BCM

Scenario 2:

- UE-> UE_ONLY
- SGSN-> UE_ONLY
- GGSN-> Mixed
- PCRF-> NO BCM

- GTP-PGW: BCM of UE_NW is considered.
- IPSG: BCM of UE_ONLY is considered.
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA: BCM of NONE is considered.

- PCC Rule Error Handling: If the installation/activation of one or more PCC rules fails, the PCEF includes one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fails, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is

generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

- Time of the Day Procedures: PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.



Important

In 11.0 and later releases, Rule-Activation-Time / Rule-Deactivation-Time / Revalidation-Time AVP is successfully parsed only if its value corresponds to current time or a later time than the current IPSPG time, else the AVP and entire message is rejected. In earlier releases the AVP is successfully parsed only if its value corresponds to a later time than the current IPSPG time, else the AVP and entire message is rejected.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).



Important

This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx: The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also be parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

Charging Control

Charging Control is the process of associating packets belonging to a SDF to a charging key, and applying online charging and/or offline charging, as appropriate. Flow-based charging handles differentiated charging of the bearer usage based on real time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, and then no offline charging information is generated.

Supported Features:

- Provisioning of Charging-related Information for the IP-CAN Session.
- Provisioning of Charging Addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses or the peer names).

**Important**

In this release, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

For the purpose of charging correlation between SDF level and application level (for example, IMS) as well as on-line charging support at the application level, applicable charging identifiers and IP-CAN type identifiers are passed from the PCRF to the AF, if such identifiers are available.

For IMS bearer charging, the IP Multimedia Core Network (IM CN) subsystem and the Packet Switched (PS) domain entities are required to generate correlated charging data.

In order to achieve this, the Gateway provides the GGSN Charging Identifier (GCID) associated with the PDP context along with its address to the PCRF. The PCRF in turn sends the IMS Charging Identifier (ICID), which is provided by the P-CSCF, to the Gateway. The Gateway generates the charging records including the GCID as well as the ICID if received from PCRF, so that the correlation of charging data can be done with the billing system.

PCRF also provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF.
 - Select downlink IP CAN bearers based on SDF filters in the PCC rule.
 - Enforce uplink IP flows are transported in the correct IP CAN bearer using the SDF filters within the PCC rule.
- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- **Dynamic PCC Rules:** Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be installed, modified, and removed at any time.
- **Predefined PCC Rule:** Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.



Important

A third type of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- **Rule Name:** The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- **Service Identifier:** The service identifier is used to identify the service or the service component the SDF relates to.
- **Service Data Flow Filter(s):** The service flow filter(s) is used to select the traffic for which the rule applies.
- **Precedence:** For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- **Gate Status:** The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- **QoS Parameters:** The QoS information includes the QoS class identifier (authorized QoS class for the SDF), the Allocation and Retention Priority (ARP), and authorized bitrates for uplink and downlink.



Important

In earlier releases, ECS used only the Priority-Level part of ARP byte for bearer binding, (along with QCI). Now the entire ARP byte is used for bearer binding (along with QCI). Since the capability and vulnerability bits are optional in a dynamic rule, if a dynamic rule is received without these flags, it is assumed that the capability bit is set to 1 (disabled) and vulnerability bit is set to 0 (enabled). For predefined rules, currently configuring these two flags is not supported, so as of now all predefined rules are assumed to have capability bit set to 1 (disabled) and vulnerability bit set to 0 (enabled).

- **Charging key (rating group)**
- **Other charging parameters:** The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF will report the usage related to the rule, and so on.

**Important**

In this release, configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

**Important**

ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without

a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.



Important

In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules.



Important

When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.



Important

In 11.0 and later releases, IMSA and ECS allow the PCRF to install two (or more) dynamic rules with the same precedence value. In earlier releases, for two distinct dynamic rules having the same precedence the second rule used to be rejected.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer are discarded.

Selecting a PCC Rule and IP CAN Bearer for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules.



Important

When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches a SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. The Downlink IP Packet is transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets that do not match any PCC rule of the IP CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Bearer Termination Implications
- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated (for example, for GPRS when the last PDP Context within the IP-CAN session is being terminated) the PCEF contacts the PCRF.
- Request of IP-CAN Bearer Termination: If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF apply the "Request of IP-CAN Session Termination" procedure.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP CAN specific procedures to terminate the IP CAN session. For GPRS, the GGSN send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the "Indication of IP CAN Session Termination" procedure.

In 12.0 and later releases, volume or rule information obtained from PCRF is discarded if the subscriber is going down.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature, which is supported by all products supporting Rel. 7 Gx interface.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

**Important**

In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

**Important**

Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

- 1 PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
- 2 IMSA updates the information to ECS.
- 3 Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
- 4 For session-level monitoring, the ECS maintains the amount of data usage.
- 5 For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
- 6 The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be the same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being

tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



Important

The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota

into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see [Configuring Volume Reporting over Gx](#), on page 386.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

How Rel. 7 Gx Works

This section describes how dynamic policy and charging control for subscribers works with Rel. 7 Gx interface support in GPRS/UMTS networks.

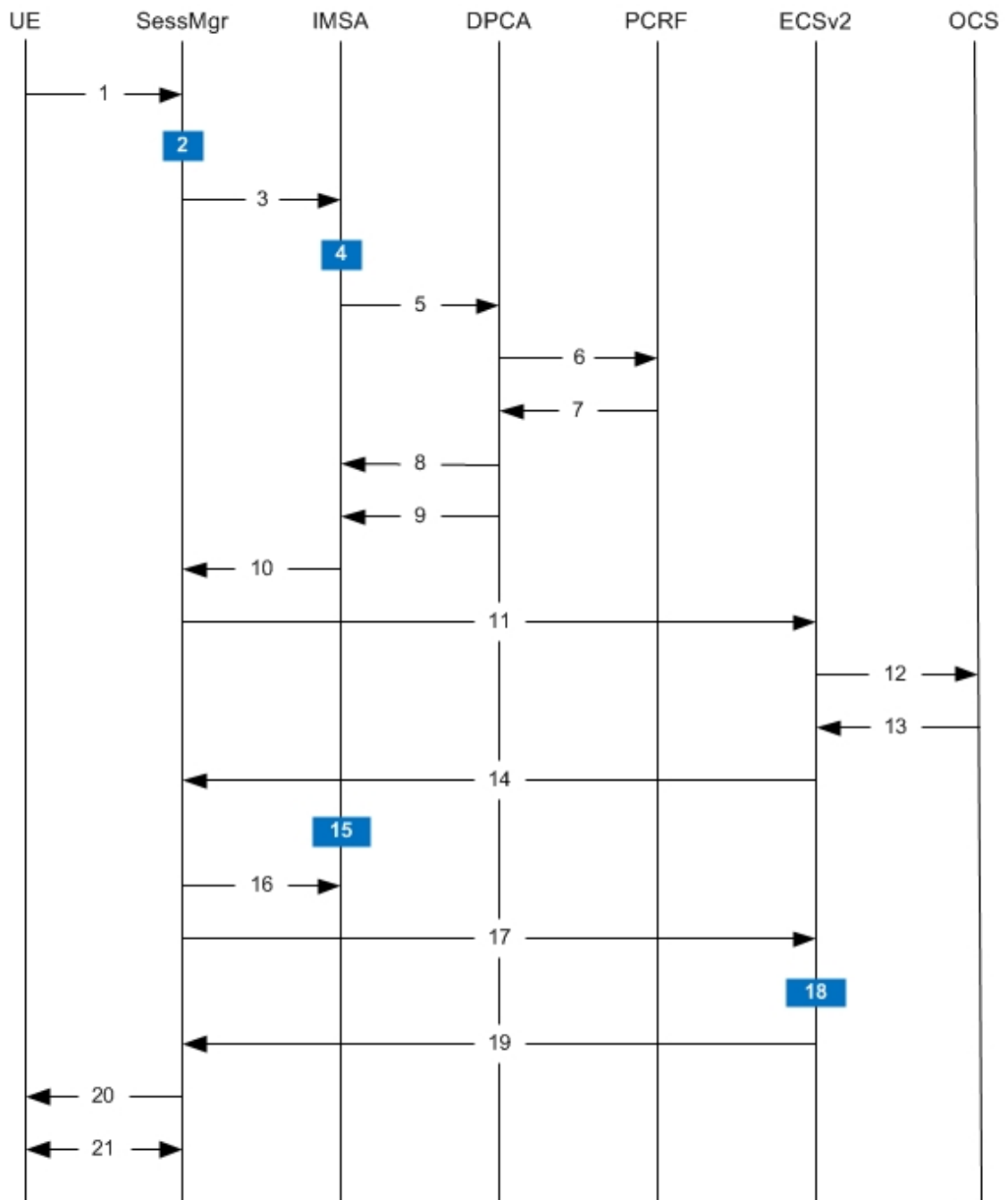
The following figure and table explain the IMSA process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

**Important**

In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 60: Rel. 7 Gx IMS Authorization Call Flow



335182

Table 26: Rel. 7 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for primary PDP context activation/creation.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the APN.
4	IMSA allocates resources for the IP CAN session and the bearer, and selects the PCRF to contact based on the user's selection key (for example, msisdn).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.
6	DPCA sends a CCR initial message to the selected PCRF. This message includes the Context-Type AVP set to PRIMARY and the IP address allocated to the UE. The message may include the Bearer-Usage AVP set to GENERAL. The Bearer-Operation is set to Establishment. The Bearer ID is included if the PCRF does the bearer binding.
7	PCRF may send preconfigured charging rules in CCA, if a preconfigured rule set for general purpose PDP context is provided in PCRF. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, and so on, along with the Bearer ID that corresponds to the rules received from the PCRF to IMSA. IMSA stores the information. If the Bearer ID is absent, and PCRF does the bearer binding, the rule is skipped. Whereas, if the Bearer ID is absent and the PCEF does the bearer binding, the rule is passed onto the ECS to perform bearer binding.
9	DPCA calls the callback function registered with it by IMSA.
10	IMSA stores the bearer authorized QoS information and notifies the SessMgr. Other PCRF provided information common to the entire PDP session (event trigger, primary/secondary OCS address, and so on) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The APN name, primary/secondary OCS server address, and so on are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the APN/AAA) and GPRS specific attributes (for example, APN, UMTS QoS, and so on).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.

Step	Description
15	SessMgr requests IMSA for the dynamic rules.
16	<p>IMSA sends the dynamic rules to SessMgr.</p> <p>Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the primary PDP context is established, all RAR messages from the PCRF were rejected.</p> <p>Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.</p>
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS. ECS performs PCEF bearer binding for rules without bearer ID.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the PDP Context Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.
21	Based on the PCEF bearer binding for the PCC rules at Step 18, the outcome could be one or more network-initiated PDP context procedures with the UE (Network Requested Update PDP Context (NRUPC) / Network Requested Secondary PDP Context Activation (NRSPCA)).

Configuring Rel. 7 Gx Interface

To configure Rel. 7 Gx interface functionality, the IMS Authorization service must be configured at the context level, and then the APN configured to use the IMS Authorization service.

To configure Rel. 7 Gx interface functionality:

-
- Step 1** Configure IMS Authorization service at the context level for IMS subscriber in GPRS/UMTS network as described in [Configuring IMS Authorization Service at Context Level](#), on page 383.
- Step 2** Verify your configuration as described in [Verifying the Configuration](#), on page 385.
- Step 3** Configure an APN within the same context to use the IMS Authorization service for IMS subscriber as described in [Applying IMS Authorization Service to an APN](#), on page 385.
- Step 4** Verify your configuration as described in [Verifying Subscriber Configuration](#), on page 386.
- Step 5** *Optional:* Configure the Volume Reporting over Gx feature as described in [Configuring Volume Reporting over Gx](#), on page 386.
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Important** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.
-

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMS Authorization service at context level for IMS subscribers in GPRS/UMTS networks:

```
configure
context <context_name>
    ims-auth-service <imsa_service_name>
        p-cscf discovery table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin
    }
        p-cscf table { 1 | 2 } row-precedence <precedence_value> { address <ip_address> | ipv6-address
<ipv6_address> } [ secondary { address <ip_address> | ipv6-address <ipv6_address> } ]
        policy-control
            diameter origin endpoint <endpoint_name>
            diameter dictionary <dictionary>
            diameter request-timeout <timeout_duration>
            diameter host-select table { { { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus |
round-robin } } [ prefix-table { 1 | 2 } }
            diameter host-select row-precedence <precedence_value> table { { { { 1 | 2 } host <host_name>
[ realm <realm_id> ] [ secondary host <host_name> [ realm <realm_id> ] ] } } [ prefix-table { 1 | 2 }
msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to> host <host_name> [
realm <realm_id> ] [ secondary host <sec_host_name> [ realm <sec_realm_id> ] algorithm {
active-standby | round-robin } ] } } [ -noconfirm ]
            diameter host-select reselect subscriber-limit <subscriber_limit> time-interval <duration>
            failure-handling cc-request-type { any-request | initial-request | terminate-request |
update-request } { diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } } { continue
| retry-and-terminate | terminate }
        end
end
```

Notes:

- `<context_name>` must be the name of the context where you want to enable IMS Authorization service.
- `<imsa_service_name>` must be the name of the IMS Authorization service to be configured for Rel. 7 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- Secondary P-CSCF IP address can be configured in the P-CSCF table. Refer to the *Command Line Interface Reference* for more information on the **p-cscf table** command.

In 18 and later releases, the syntax for **p-cscf table** configuration command is:

```
p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } ] [ weight value ]
```

- To enable Rel. 7 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- When configuring the MSISDN prefix range based PCRF selection mechanism:

To enable the Gx interface to connect to a specific PCRF for a range of subscribers configure **msisdn-prefix-from** `<msisdn_prefix_from>` and **msisdn-prefix-to** `<msisdn_prefix_to>` with the starting and ending MSISDNs respectively.

To enable the Gx interface to connect to a specific PCRF for a specific subscriber, configure both **msisdn-prefix-from** `<msisdn_prefix_from>` and **msisdn-prefix-to** `<msisdn_prefix_to>` with the same MSISDN.

In StarOS 8.1 and later releases, per MSISDN prefix range table a maximum of 128 rows can be added. In StarOS 8.0 and earlier releases, a maximum of 100 rows can be added.

The MSISDN ranges must not overlap between rows.

- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- *Optional:* To configure the Quality of Service (QoS) update timeout for a subscriber, in the IMS Authorization Service Configuration Mode, enter the following command:

```
qos-update-timeout <timeout_duration>
```



Important

This command is obsolete in release 11.0 and later releases.

- *Optional:* To configure signalling restrictions, in the IMS Authorization Service Configuration Mode, enter the following commands:

```
signaling-flag { deny | permit }
```

```
signaling-flow permit server-address <ip_address> [ server-port { <port_number> | range <start_number> to <end_number> } ] [ description <string> ]
```

- *Optional:* To configure action on packets that do not match any policy gates in the general purpose PDP context, in the IMS Authorization Service Configuration Mode, enter the following command:

```
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }
```

- To configure the PCRF host destinations configured in the GGSN/PCEF, use the **diameter host-select** CLI commands.
- To configure the GGSN/PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.
- For provisioning of default charging method, use the following configurations. For this, the AVPs Online and Offline will be sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

- To send Enable Online:

```
configure
```

```
active-charging service <ecs_service_name>
```

```
charging-action <charging_action_name>
```

```
cca charging credit
```

```
exit
```

- To send Enable Offline:

```
configure
```

```
active-charging service <ecs_service_name>
```

```
rulebase <rulebase_name>
```

```
billing-records rf
```

```
exit
```

Verifying the Configuration

To verify the IMS Authorization service configuration:

-
- | | |
|---------------|--|
| Step 1 | Change to the context where you enabled IMS Authorization service by entering the following command:
context <context_name> |
| Step 2 | Verify the IMS Authorization service's configurations by entering the following command:
show ims-authorization service name <imsa_service_name> |
-

Applying IMS Authorization Service to an APN

After configuring IMS Authorization service at the context-level, an APN must be configured to use the IMS Authorization service for an IMS subscriber.

Use the following example to apply IMS Authorization service functionality to a previously configured APN within the context configured as described in [Configuring Rel. 7 Gx Interface](#), on page 382.

```
configure
context <context_name>
  apn <apn_name>
    ims-auth-service <imsa_service_name>
    active-charging rulebase <rulebase_name>
  end
```

Notes:

- <context_name> must be the name of the context in which the IMS Authorization service was configured.
- <imsa_service_name> must be the name of the IMS Authorization service configured for IMS authentication in the context.
- For Rel. 7 Gx, the ECS rulebase must be configured in the APN.
- ECS allows change of rulebase via Gx for PCEF binding scenarios. When the old rulebase goes away, all the rules that were installed from that rulebase are removed. This may lead to termination of a few bearers (PDP contexts) if they are left without any rules. If there is a Gx message that changes the rulebase, and also activates some predefined rules, the rulebase change is made first, and the rules are activated from the new rulebase. Also, the rulebase applies to the entire call. All PDP contexts (bearers) in one call use the same ECS rulebase.
- For predefined rules configured in the ECS, MBR/GBR of a dynamic/predefined rule is checked before it is used for PCEF binding. All rules (dynamic as well as predefined) have to have an MBR associated with them and all rules with GBR QCI should have GBR also configured. So for predefined rules, one needs to configure appropriate peak-data-rate, committed-data-rate as per the QCI being GBR QCI or non-GBR QCI. For more information, in the ACS Charging Action Configuration Mode, see the **flow limit-for-bandwidth** CLI command.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

```
policy-control charging-rule-base-name active-charging-group-of-ruledefs
```

Verifying Subscriber Configuration

Verify the IMS Authorization service configuration for subscriber(s) by entering the following command:

```
show subscribers ims-auth-service <imsa_service_name>
```

<imsa_service_name> must be the name of the IMS Authorization service configured for IMS authentication.

Configuring Volume Reporting over Gx

This section describes the configuration required to enable Volume Reporting over Gx.

To enable Volume Reporting over Gx, use the following configuration:

```
configure
  active-charging service <ecs_service_name>
    rulebase <rulebase_name>
      action priority <priority> dynamic-only ruledef <ruledef_name> charging-action
        <charging_action_name> monitoring-key <monitoring_key>
```

```

    exit
  exit
  context <context_name>
    ims-auth-service <imsa_service_name>
      policy-control
        event-update send-usage-report [ reset-usage ]
      end
    end
  end
end

```

Notes:

- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI which enables volume usage report to be sent in event updates is available only in 10.2 and later releases. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the usage information as part of event update but not reset at PCEF.

Gathering Statistics

This section explains how to gather Rel. 7 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Table 27: Gathering Rel. 7 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	show ims-authorization policy-control statistics
Information and statistics specific to the authorization servers used for IMS Authorization service.	show ims-authorization servers ims-auth-service
Information of all IMS Authorization service.	show ims-authorization service all
Statistics of IMS Authorization service.	show ims-authorization service statistics
Information, configuration, and statistics of sessions active in IMS Authorization service.	show ims-authorization sessions all
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	show ims-authorization sessions full
Summarized information of sessions active in IMS Authorization service.	show ims-authorization sessions summary
Complete statistics for active charging service sessions.	show active-charging sessions full

Statistics/Information	Action to perform
Information for all rule definitions configured in the service.	show active-charging ruledef all
Information for all rulebases configured in the system.	show active-charging rulebase all
Information on all group of ruledefs configured in the system.	show active-charging group-of-ruledefs all
Information on policy gate counters and status.	show ims-authorization policy-gate { counters status } This command is no longer an option in StarOS release 11.0 and beyond.

Rel. 8 Gx Interface

Rel. 8 Gx interface support is available on the Cisco ASR chassis running StarOS 10.0 or StarOS 11.0 and later releases.

This section describes the following topics:

- [HA/PDSN Rel. 8 Gx Interface Support, on page 388](#)
- [P-GW Rel. 8 Gx Interface Support, on page 406](#)

HA/PDSN Rel. 8 Gx Interface Support

This section provides information on configuring Rel. 8 Gx interface for HA and PDSN to support policy and charging control for subscribers in CDMA networks.

The IMS service provides application support for transport of voice, video, and data independent of access support. Roaming IMS subscribers in CDMA networks require apart from other functionality sufficient, uninterrupted, consistent, and seamless user experience during an application session. It is also important that a subscriber gets charged only for the resources consumed by the particular IMS application used.

It is recommended that before using the procedures in this section you select the configuration example that best meets your service model, and configure the required elements for that model as described in this Administration Guide.

This section describes the following topics:

- [Introduction, on page 389](#)
- [Terminology and Definitions, on page 391](#)
- [How it Works, on page 398](#)
- [Configuring HA/PDSN Rel. 8 Gx Interface Support, on page 402](#)
- [Gathering Statistics, on page 405](#)

Introduction

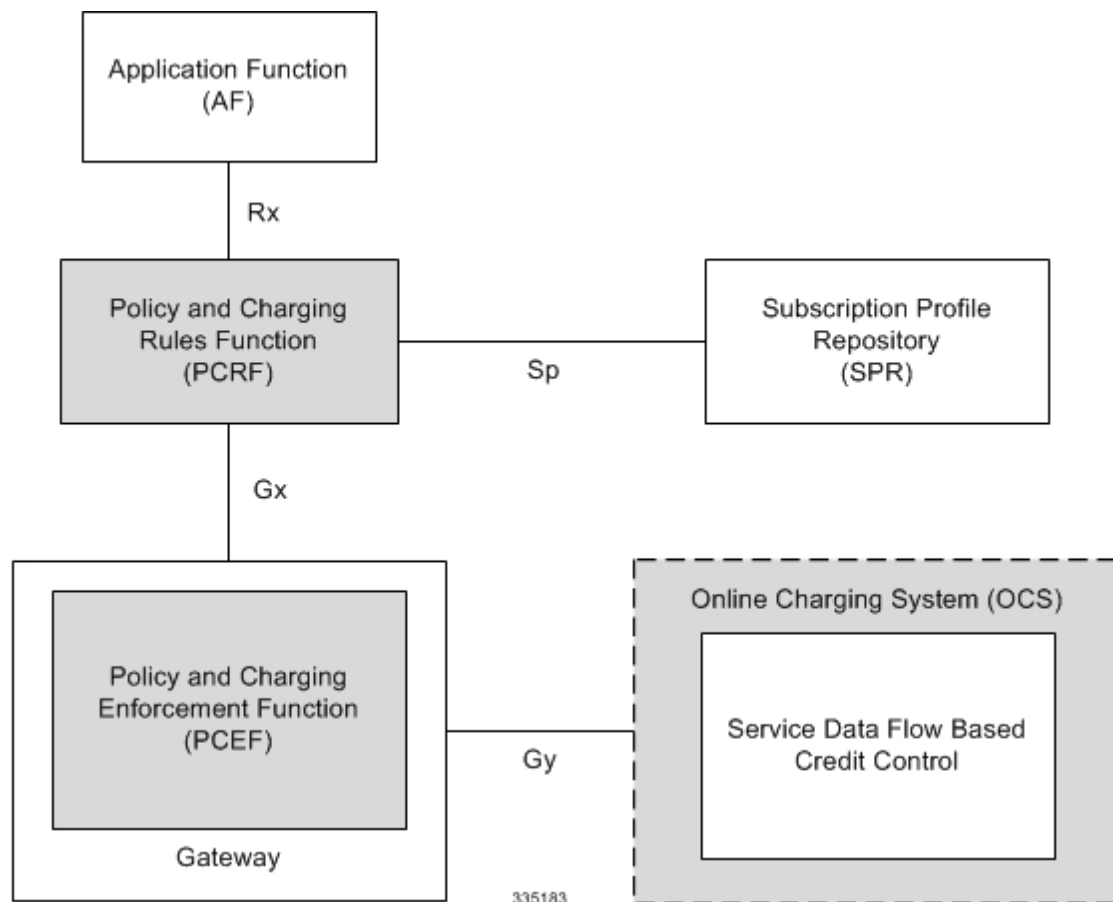
For IMS deployment in CDMA networks the system uses Rel. 8 Gx interface for policy-based admission control support and flow-based charging (FBC). The Rel. 8 Gx interface supports enforcing policy control features like gating, bandwidth limiting, and so on, and also supports FBC. This is accomplished via dynamically provisioned Policy Control and Charging (PCC) rules. These PCC rules are used to identify Service Data Flows (SDF) and to do charging. Other parameters associated with the rules are used to enforce policy control.

The PCC architecture allows operators to perform service-based QoS policy and FBC control. In the PCC architecture, this is accomplished mainly by the Policy and Charging Enforcement Function (PCEF)/HA/PDSN and the Policy and Charging Rules Function (PCRF). The client functionality lies with the HA/PDSN, therefore in the IMS Authorization (IMSA) scenario it is also called the Gateway. The PCEF function is provided by the Enhanced Charging Service (ECS). The Gx interface is implemented as a Diameter connection. The Gx messaging mostly involves installing/modifying/removing dynamic rules and activating/deactivating predefined rules.

The Gx reference point is located between the Gateway/PCEF and the PCRF. This reference point is used for provisioning and removal of PCC rules from the PCRF to the Gateway/PCEF, and the transmission of traffic plane events from the Gateway/PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both by applying AVPs relevant to the application.

The following figure shows the reference points between elements involved in the policy and charging architecture.

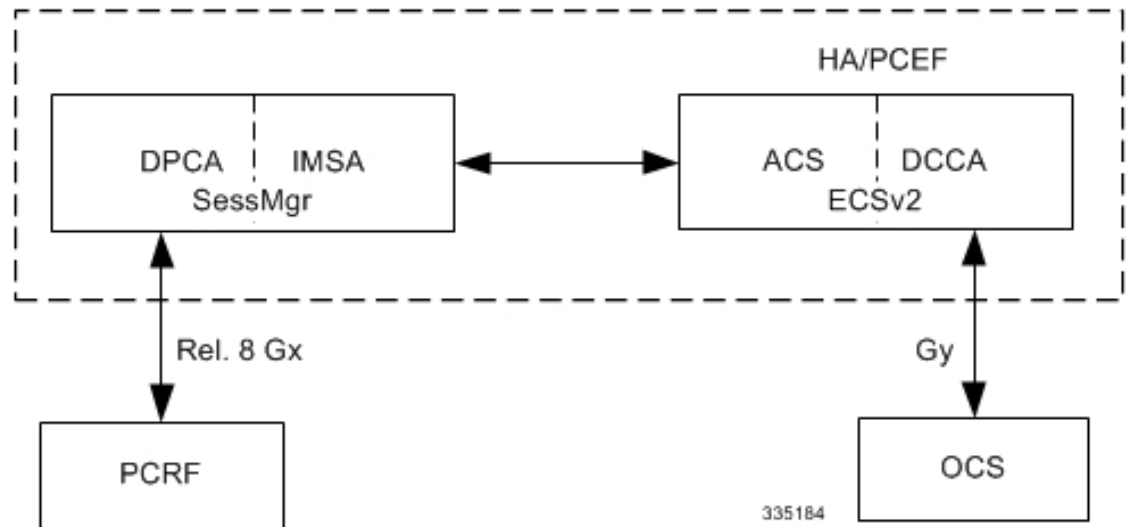
Figure 61: HA/PDSN Rel. 8 Gx PCC Logical Architecture



Within the Gateway, the IMSA and DPCA modules handle the Gx protocol related functions (at the SessMgr) and the policy enforcement and charging happens at ECS. The Gy protocol related functions are handled within the DCCA module (at the ECS).

The following figure shows the interaction between components within the Gateway.

Figure 62: HA/PDSN Rel. 8 Gx PCC Architecture within PCEF



License Requirements

The HA/PDSN Rel. 8 Gx interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Supported Standards

HA/PDSN Rel 8. Gx interface support is based on the following standards and RFCs:

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588, Diameter Base Protocol; September 2003
- RFC 4006, Diameter Credit-Control Application; August 2005

Terminology and Definitions

This section describes features and terminology pertaining to HA/PDSN Rel. 8 Gx functionality.

Policy Control

The process whereby the PCRF indicates to the PCEF how to control the IP-CAN session.

Policy control comprises the following functions:

- Binding
- Gating Control
- Event Reporting
- QoS Control
- Other Features



Binding

In the HA/PDSN Rel. 8 Gx implementation, since there are no bearers within a MIP session the IP-CAN Bearer concept does not apply. Only authorized IP-CAN session is applicable.

Gating Control

Gating control is the blocking or allowing of packets belonging to an SDF, to pass through to the desired endpoint. A gate is described within a PCC rule and gating control is applied on a per SDF basis. The commands to open or close the gate leads to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed, all packets of the related IP flows are dropped. If the gate is open, the packets of the related IP flows are allowed to be forwarded.


Event Reporting

 Important	<hr/> Unconditional reporting of event triggers from PCRF to PCEF when PCEF has not requested for is not supported. <hr/>
 Important	<hr/> In the HA/PDSN Rel. 8 Gx implementation, only the AN_GW_CHANGE (21) event trigger is supported. <hr/>

Event reporting is the notification of and reaction to application events to trigger new behavior in the user plane as well as the reporting of events related to the resources in the Gateway (PCEF). Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Event trigger reporting from PCEF to PCRF, and provisioning of event triggers happens at IP-CAN session level.

The Event Reporting Function (ERF) located in the PCEF, receives event triggers from PCRF during the Provision of PCC Rules procedure and performs event trigger detection. When an event matching the received event trigger occurs, the ERF reports the occurred event to the PCRF. If the provided event triggers are associated with certain parameter values then the ERF includes those values in the response to the PCRF.

QoS Control

 Important	<hr/> In the HA/PDSN Rel. 8 Gx implementation, only authorized IP-CAN Session is supported. Provisioning of authorized QoS per IP-CAN bearer, policy enforcement for authorized QoS per QCI, and coordination of authorized QoS scopes in mixed mode are not applicable. <hr/>
---	--

QoS control is the authorization and enforcement of the maximum QoS that is authorized for an SDF. In case of an aggregation of multiple SDFs, the combination of the authorized QoS information of the individual SDFs is provided as the authorized QoS for this aggregate. QoS control per SDF allows the PCC architecture to provide the PCEF with the authorized QoS to be enforced for each specific SDF.

QoS authorization information may be dynamically provisioned by the PCRF, or it can be a predefined PCC rule in the PCEF. For a predefined PCC rule within the PCEF, the authorized QoS information takes affect when the PCC rule is activated. The PCEF combines the different sets of authorized QoS information, that is the information received from the PCRF and the information corresponding to the predefined PCC rules. The PCRF knows the authorized QoS information of the predefined PCC rules and takes this information into account when activating them. This ensures that the combined authorized QoS of a set of PCC rules that are activated by the PCRF is within the limitations given by the subscription and operator policies regardless of whether these PCC rules are dynamically provided, predefined, or both.

Supported features include:

- Provisioning and Policy Enforcement of Authorized QoS: The PCRF may provide authorized QoS to the PCEF. The authorized QoS provides appropriate values for resources to be enforced.
- Policy Provisioning for Authorized QoS Per SDF: The provisioning of authorized QoS per SDF is a part of PCC rule provisioning procedure.
- Policy Enforcement for Authorized QoS Per SDF: If an authorized QoS is defined for a PCC rule, the PCEF limits the data rate of the SDF corresponding to that PCC rule not to exceed the maximum authorized bandwidth for the PCC rule by discarding packets exceeding the limit.
- Upon deactivation or removal of a PCC rule, the PCEF frees the resources reserved for that PCC rule.

Other Features

This section describes some of the other features.

PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF communicates the failure to the PCRF by including one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF identifies the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), identifies the failed reason code by including a Rule-Failure-Code AVP, and includes the PCC-Rule-Status AVP.

If the installation/activation of one or more new PCC rules (that is, rules that were not previously successfully installed) fail, the PCEF sets the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF sends the PCRF a new CCR command and includes the Charging-Rule-Report AVP. The PCEF includes the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and sets the PCC-Rule-Status to INACTIVE.

In releases prior to 18, P-GW/GGSN does not send CCR-U with Charging Rule report for rule binding failure occurred during 4G to 3G HO in a collision case where create/update bearer response in 3G/4G is pending and update bearer of 3G HO is received. In 18 and later releases, CCR-U is generated and sent to PCRF for reporting rule failure when the collision happens during GnGp HO scenario.

This additional Gx message (CCR-U) triggered will require multiple CCR-Us to be configured when RAT_TYPE trigger is enabled. Otherwise, the subscriber call will be dropped whenever the collision happens during HO.

In the HA/PDSN Gx implementation, the following rule failure codes are supported:

- RATING_GROUP_ERROR (2)

- SERVICE_IDENTIFIER_ERROR (3)
- GW/PCEF_MALFUNCTION (4)
- RESOURCES_LIMITATION (5)

If the installation/activation of one or more PCC rules fails during RAR procedure, the RAA command is sent with the Experimental-Result-Code AVP set to DIAMETER_PCC_RULE_EVENT (5142).

Time of the Day Procedures

PCEF performs PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, causes the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP-CAN session. The PCEF stops the timer once the PCEF triggers a REVALIDATION_TIMEOUT event.

When installed, the PCC rule is inactive. If Rule-Activation-Time / Rule-Deactivation-Time is specified, then the PCEF sets the rule active / inactive after that time.

In releases prior to 17.0, if "Rule-Deactivation-Time" AVP for a predefined rule was omitted in a CCA-U or RAR message, then any previous value for this AVP was continued to be used in the chassis. In 17.0 and later releases, if Rule-Deactivation-Time AVP is omitted in CCA/RAR, then any previous value for this AVP is no longer valid. The new behavior is compliant to the 3GPP specification for Gx, version 12.1.0.

If PCRF enables the same predefined rule again in RAR/CCA-U without Rule-Deactivation-Time AVP, then the deactivation-time for this rule, if any, will be removed.

For switching to the old behavior, PCRF should re-send the same value of Rule-Deactivation-Time AVP along with predef-rule name in the PCRF message (RAR, CCA-U).



Note

This behavior change is applicable only to predefined rules.

Support for Firewall Policy on Gx

The Diameter AVP "SN-Firewall-Policy" has been added to the Diameter dynamic dictionary to support Firewall policy on Gx interface. This AVP can be encoded in CCA-I message to apply/overwrite the fw-and-nat policy that has either been statically assigned to the PDP context via APN configuration or dynamically assigned via RADIUS in Access-Accept. This AVP can also be parsed in any CCA-U or RAR message to modify the fw-and-nat policy that is currently assigned to the PDP context.

Charging Control



Important

In the HA/PDSN Rel. 8 Gx implementation, offline charging is not supported.

Charging Control is the process of associating packets belonging to an SDF to a charging key, and applying online charging as appropriate. FBC handles differentiated charging of the bearer usage based on real-time analysis of the SDFs. In order to allow for charging control, the information in the PCC rule identifies the SDF and specifies the parameters for charging control. The PCC rule information may depend on subscription data.

Online charging is supported via the Gy interface. In the case of online charging, it is possible to apply an online charging action upon PCEF events (for example, re-authorization upon QoS change).

It is possible to indicate to the PCEF that interactions with the charging systems are not required for a PCC rule, that is to perform neither accounting nor credit control for this SDF, then neither online nor offline charging is performed.

Supported Features:

- Provisioning of charging-related information for the IP-CAN Session
- Provisioning of charging addresses: Primary or secondary event charging function name (Online Charging Server (OCS) addresses)



Important

In the HA/PDSN Rel. 8 Gx implementation, provisioning of primary or secondary charging collection function name (Offline Charging Server (OFCS) addresses) over Gx is not supported.

- Provisioning of Default Charging Method: In this release, the default charging method is sent in CCR-I message. For this, new AVPs Online/Offline are sent in CCR-I message based on the configuration. The Online/Offline AVP received at command level applies only to dynamic rules if they are not configured at PCC rule level.

Charging Correlation

In the HA/PDSN Rel. 8 Gx implementation, Charging Correlation is not supported. PCRF provides the flow identifier, which uniquely identifies an IP flow in an IMS session.

Policy and Charging Control (PCC) Rules

A PCC rule enables the detection of an SDF and provides parameters for policy control and/or charging control. The purpose of the PCC rule is to:

- Detect a packet belonging to an SDF in case of both uplink and downlink IP flows based on SDF filters in the PCC rule (packet rule matching).

If no PCC rule matches the packet, the packet is dropped.

- Identify the service that the SDF contributes to.
- Provide applicable charging parameters for an SDF.
- Provide policy control for an SDF.

The PCEF selects a PCC rule for each packet received by evaluating received packets against SDF filters of PCC rules in the order of precedence of the PCC rules. When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied.

There are two types of PCC rules:

- Dynamic PCC Rules: Rules dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified, and deactivated at any time.
- Predefined PCC Rule: Rules preconfigured in the PCEF by the operators. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

**Important**

A third kind of rule, the static PCC rule can be preconfigured in the chassis by the operators. Static PCC rules are not explicitly known in the PCRF, and are not under control of the PCRF. Static PCC rules are bound to general purpose bearer with no Gx control.

A PCC rule consists of:

- Rule Name: The rule name is used to reference a PCC rule in the communication between the PCEF and PCRF.
- Service Identifier: The service identifier is used to identify the service or the service component the SDF relates to.
- Service Data Flow Filter(s): The service flow filter(s) is used to select the traffic for which the rule applies.
- Precedence: For different PCC rules with overlapping SDF filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same priority, the dynamic PCC rule takes precedence.
- Gate Status: The gate status indicates whether the SDF, detected by the SDF filter(s), may pass (gate is open) or will be discarded (gate is closed) in uplink and/or in downlink direction.
- QoS Parameters: The QoS information includes the QoS class identifier (authorized QoS class for the SDF), and authorized bitrates for uplink and downlink.
- Charging Key (rating group)
- Other charging parameters: The charging parameters define whether online charging interfaces are used, on what level the PCEF will report the usage related to the rule, etc.

**Important**

Configuring the Metering Method and Reporting Level for dynamic PCC rules is not supported.

PCC rules also include Application Function (AF) record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS, this includes the IMS Charging Identifier (ICID) and flow identifiers.

**Important**

ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

In releases prior to 14.0, there were only 10 PCC rules that were recovered per bearer in the event of a session manager crash. In 14.0 and later releases, this limit has been increased to 24. That is, up to 24 PCC rules can be recovered post ICSR.

With the increase in the limit of PCC rules that can be recovered, the rules are not lost and hence the charging applied to the end users are not impacted.

In releases prior to 17.0, when P-GW received PCC rules from PCRF and it results in Create Bearer or Update Bearer to be triggered towards MME/S-GW, the PCC rules were kept in a pending-active state. Any modification request that was received for these pending-active rules were not currently honored by the P-GW. In 17.0 and later releases, when modification for the PCC rules in pending-active state is received, the modified parameters will be buffered at P-GW. After the response for the pending request is received from the access

network, P-GW will process the modification of the buffered parameters and if required generate another update towards network.

PCC Procedures over Gx Reference Point

Request for PCC Rules

The PCEF, via the Gx reference point, requests for PCC rules in the following instances:

- At IP-CAN session establishment
- At IP-CAN session modification

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an event trigger.

Provisioning of PCC Rules

The PCRF indicates, via the Rel. 8 Gx reference point, the PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL (provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, the PCRF provisions PCC rules in the CC-Answer.
- PUSH (unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF. For example, in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF includes these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon unsolicited provisioning, the PCRF provisions zero or more PCC rules. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF provisions a reference to this PCC rule within a Charging-Rule-Name AVP and indicates the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.
- To install or modify a PCRF-provisioned PCC rule, the PCRF provisions a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.
- To remove a PCC rule which has previously been provisioned by the PCRF, the PCRF provisions the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.



Important

In 11.0 and later releases, the maximum valid length for a charging rule name is 63 bytes. When the length of the charging rule name is greater than 63 bytes, a charging rule report with RESOURCES_LIMITATION as Rule-Failure-Code is sent. This charging rule report is sent only when the length of the rule name is lesser than 128 characters. When the charging rule name length is greater than or equal to 128 characters no charging rule report will be sent. In earlier releases, the length of the charging rule name constructed by PCRF was limited to 32 bytes.

Releases prior to 14.0, when PCRF has subscribed to Out of Credit trigger, on session connect when one rule validation fails and also when an Out of Credit was received from OCS for another rule, P-GW was trying to report these failures in different CCR-U to PCRF. However, the second CCR-U of Out of credit was getting dropped internally.

In 14.0 and later releases, on session connect, P-GW combines the rule failure and out of credit in the same CCR-U and sends to PCRF.

Selecting a PCC Rule for Uplink IP Packets

If PCC is enabled, the PCEF selects the applicable PCC rule for each received uplink IP packet within an IP-CAN session by evaluating the packet against uplink SDF filters of PCRF-provided or predefined active PCC rules of this IP-CAN session in the order of the precedence of the PCC rules.



Important

When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink SDF filters of the PCRF-provided PCC rule is applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Uplink IP packets which do not match any PCC rule of the corresponding IP-CAN session are discarded.

Selecting a PCC Rule for Downlink IP Packets

If PCC is enabled, the PCEF selects a PCC rule for each received downlink IP packet within an IP-CAN session by evaluating the packet against downlink SDF filters of PCRF-provided or predefined active PCC rules of the IP-CAN session in the order of precedence of the PCC rules.



Important

When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink SDF filters of the PCRF-provided PCC rule are applied first.

When a packet matches an SDF filter, the packet matching process for that packet is completed, and the PCC rule for that filter is applied. Downlink IP packets that do not match any PCC rule of the IP-CAN session are discarded.

The following procedures are also supported:

- Indication of IP-CAN Session Termination: When the IP-CAN session is being terminated the PCEF contacts the PCRF.
- Request of IP-CAN Session Termination: If the PCRF decides to terminate an IP-CAN session due to an internal trigger or trigger from the SPR, the PCRF informs the PCEF. The PCEF acknowledges to the PCRF and instantly removes/deactivates all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF applies IP-CAN specific procedures to terminate the IP-CAN session. The HA/PDSN sends a MIP Revocation Request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested. Furthermore, the PCEF applies the "Indication of IP-CAN Session Termination" procedure.
- Use of the Supported-Features AVP during session establishment to inform the destination host about the required and optional features that the origin host supports.

How it Works

This section describes how HA/PDSN Rel. 8 Gx Interface support works.

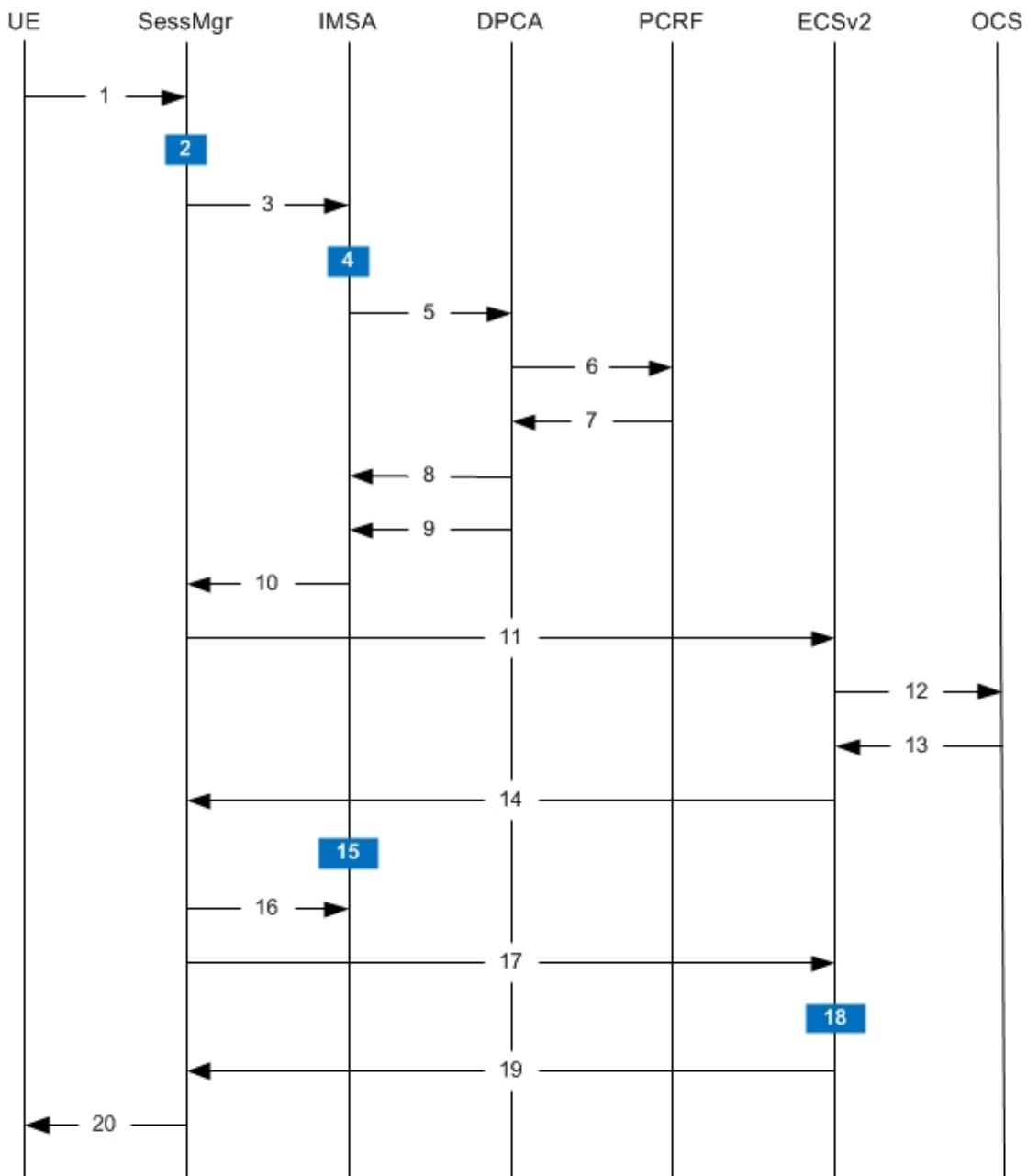
The following figure and table explain the IMS Authorization process between a system and IMS components that is initiated by the UE.

In this example, the Diameter Policy Control Application (DPCA) is the Gx interface to the PCRF. The interface between IMSA with PCRF is the Gx interface, and the interface between Session Manager (SessMgr) and Online Charging Service (OCS) is the Gy interface. Note that the IMSA service and DPCA are part of SessMgr on the system and separated in the figure for illustration purpose only.

**Important**

In 14.0 and later releases, the DPCA and the IMSA will be acting as one module within the Policy Server interface application.

Figure 63: HA/PDSN Rel. 8 Gx IMS Authorization Call Flow



335185

Table 28: HA/PDSN Rel. 8 Gx IMS Authorization Call flow Description

Step	Description
1	UE (IMS subscriber) requests for MIP Registration Request.
2	SessMgr allocates an IP address to the UE.
3	SessMgr requests IMS Authorization, if IMSA is enabled for the subscriber. IMSA service can either be configured in the subscriber template, or can be received from the AAA.
4	IMSA allocates resources for the IP-CAN session, and selects the PCRF to contact based on the user's selection key (for example, round-robin).
5	IMSA requests the DPCA module to issue an auth request to the PCRF.
6	DPCA sends a CCR initial message to the selected PCRF.
7	PCRF may send preconfigured charging rules in CCA. The dynamic rules and the authorized QoS parameters could also be included by the PCRF.
8	DPCA passes the charging rule definition, charging rule install, QoS information received from the PCRF, event triggers, etc. IMSA stores the information.
9	DPCA calls the callback function registered with it by IMSA.
10	PCRF-provided information common to the entire IP-CAN session (event trigger, primary/secondary OCS address, etc.) is stored within the IMSA. After processing the information, IMSA notifies the SessMgr about the policy authorization complete.
11	If the validation of the rules fails in IMSA/DPCA, a failure is notified to PCRF containing the Charging-Rule-Report AVP. Else, IMSA initiates creation of ECS session. The primary/secondary OCS server address, etc. are sent to the ECS from the SessMgr.
12	ECS performs credit authorization by sending CCR(I) to OCS with CC-Request-Type set to INITIAL_REQUEST to open the credit control session. This request includes the active Rulebase-Id (default rulebase ID from the AAA).
13	OCS returns a CCA initial message that may activate a statically configured Rulebase and may include preemptive quotas.
14	ECS responds to SessMgr with the response message.
15	SessMgr requests IMSA for the dynamic rules.

Step	Description
16	<p>IMSA sends the dynamic rules to SessMgr.</p> <p>Note that, in 14.0 and later releases, the RAR messages are allowed before the session is established. In earlier releases, until the MIP session is established, all RAR messages from the PCRF were rejected.</p> <p>Also note that, in 14.0 and later releases, the RAR message is rejected and RAA is sent with 3002 result code when the recovery of dynamic rule information and audit of Session Manager are in progress. Earlier, the RAR messages were processed by DPCA even when the recovery audit was in progress.</p>
17	SessMgr sends the dynamic rule information to the ECS. The gate flow status information and the QoS per flow (charging rule) information are also sent in the message.
18	ECS activates the predefined rules received, and installs the dynamic rules received. Also, the gate flow status and the QoS parameters are updated by ECS as per the dynamic charging rules. The Gx rulebase is treated as an ECS group-of-ruledefs. The response message contains the Charging Rule Report conveying the status of the rule provisioning at the ECS.
19	If the provisioning of rules fails partially, the context setup is accepted, and a new CCR-U is sent to the PCRF with the Charging-Rule-Report containing the PCC rule status for the failed rules. If the provisioning of rules fails completely, the context setup is rejected.
20	Depending on the response for the MIP Session Authorization, SessMgr sends the response to the UE and activates/rejects the call. If the Charging-Rule-Report contains partial failure for any of the rules, the PCRF is notified, and the call is activated. If the Charging-Rule-Report contains complete failure, the call is rejected.

Configuring HA/PDSN Rel. 8 Gx Interface Support

To configure HA/PDSN Rel. 8 Gx Interface functionality:

- 1 At the context level, configure IMSA service for IMS subscribers as described in [Configuring IMS Authorization Service at Context Level](#), on page 403.
- 2 Within the same context, configure the subscriber template to use the IMSA service as described in [Applying IMS Authorization Service to Subscriber Template](#), on page 404.
- 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



Important

Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring IMS Authorization Service at Context Level

Use the following example to configure IMSA service at context level for IMS subscribers:

```
configure
context <context_name>
  ims-auth-service <imsa_service_name>
  policy-control
    diameter origin endpoint <endpoint_name>
    diameter dictionary <dictionary>
    diameter request-timeout <timeout_duration>
    diameter host-select table { 1 | 2 } algorithm round-robin
    diameter host-select row-precedence <precedence_value> table { 1 | 2 } host
    <primary_host_name> [ realm <primary_realm_id> ] [ secondary host <secondary_host_name> [ realm
    <secondary_realm_id> ] ] [ -noconfirm ]
    failure-handling cc-request-type { any-request | initial-request | terminate-request |
update-request } { diameter-result-code { any-error | <result_code> [ to <end_result_code> ] } } { continue
| retry-and-terminate | terminate }
  exit
  exit
  diameter endpoint <endpoint_name> [ -noconfirm ]
  origin realm <realm_name>
  use-proxy
  origin host <host_name> address <ip_address>
  no watchdog-timeout
  response-timeout <timeout_duration>
  connection timeout <timeout_duration>
  connection retry-timeout <timeout_duration>
  peer <primary_peer_name> [ realm <primary_realm_name> ] address <ip_address> [ port
<port_number> ]
  peer <secondary_peer_name> [ realm <secondary_realm_name> ] address <ip_address> [ port
<port_number> ]
  end
```

Notes:

- <context_name> must be the name of the context where you want to enable IMSA service.
- <imsa_service_name> must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.
- In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.
- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- To configure the PCRF host destinations configured in the PCEF, use the **diameter host-select** CLI command.
- To configure the PCEF to use a pre-defined rule when the Gx fails, set the **failure-handling cc-request-type** CLI to **continue**. Policies available/in use will continue to be used and there will be no further interaction with the PCRF.

Verifying the IMSA Service Configuration

To verify the IMSA service configuration:

- 1 Change to the context where you enabled IMSA service by entering the following command:
context <context_name>
- 2 Verify the IMSA service configuration by entering the following command:
show ims-authorization service name <imsa_service_name>

Applying IMS Authorization Service to Subscriber Template

After configuring IMSA service at the context-level, within the same context subscriber template must be configured to use the IMSA service for IMS subscribers.

Use the following example to apply IMSA service functionality to subscriber template within the context configured as described in [Configuring IMS Authorization Service at Context Level](#), on page 403.

```
configure
context <context_name>
  subscriber default
    encrypted password <encrypted_password>
    ims-auth-service <imsa_service_name>
    ip access-group <access_group_name> in
    ip access-group <access_group_name> out
    ip context-name <context_name>
    mobile-ip home-agent <ip_address>
    active-charging rulebase <rulebase_name>
  end
```

Notes:

- <context_name> must be the name of the context in which the IMSA service was configured.
- <imsa_service_name> must be the name of the IMSA service configured for IMS authentication in the context.
- The ECS rulebase must be configured in the subscriber template.
- For interpretation of the Gx rulebase (Charging-Rule-Base-Name AVP) from PCRF as ECS group-of-ruledefs, configure the following command in the Active Charging Service Configuration Mode:

```
policy-control charging-rule-base-name active-charging-group-of- ruledefs
```

Verifying the Subscriber Configuration

Verify the IMSA service configuration for subscriber(s) by entering the following command in the Exec CLI configuration mode:

```
show subscribers ims-auth-service <imsa_service_name>
```

Notes:

- <imsa_service_name> must be the name of the IMSA service configured for IMS authentication.

Gathering Statistics

This section explains how to gather Rel. 8 Gx statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Table 29: Gathering HA/PDSN Rel. 8 Gx Statistics and Information

Statistics/Information	Action to perform
Information and statistics specific to policy control in IMS Authorization service.	show ims-authorization policy-control statistics
Information and statistics specific to the authorization servers used for IMS Authorization service.	show ims-authorization servers ims-auth-service
Information of all IMS Authorization service.	show ims-authorization service all
Statistics of IMS Authorization service.	show ims-authorization service statistics
Information, configuration, and statistics of sessions active in IMS Authorization service.	show ims-authorization sessions all
Complete information, configuration, and statistics of sessions active in IMS Authorization service.	show ims-authorization sessions full
Summarized information of sessions active in IMS Authorization service.	show ims-authorization sessions summary
Complete statistics for active charging service sessions.	show active-charging sessions full
Information for all rule definitions configured in the service.	show active-charging ruledef all
Information for all rulebases configured in the system.	show active-charging rulebase all
Information on all group of ruledefs configured in the system.	show active-charging group-of-ruledefs all
Information on policy gate counters and status.	show ims-authorization policy-gate { counters status } This command is no longer an option in StarOS release 11.0 and beyond.

P-GW Rel. 8 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 8 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.



Important

In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.



Important

Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

- 1 PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
- 2 IMSA updates the information to ECS.
- 3 Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
- 4 For session-level monitoring, the ECS maintains the amount of data usage.
- 5 For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
- 6 The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped

on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In

12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



Important

The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to [Configuring Volume Reporting over Gx](#), on page 386.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Rel. 9 Gx Interface

Rel. 9 Gx interface support is available on the Cisco ASR chassis running StarOS 12.2 and later releases.

P-GW Rel. 9 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF reports to the PCRF when the status of the related service data flow changes.
- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.



Important

ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 9 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 9 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.



Important

In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V9.5.0 (2011-01): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.



Important

Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

- 1 PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
- 2 IMSA updates the information to ECS.
- 3 Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
- 4 For session-level monitoring, the ECS maintains the amount of data usage.

- 5 For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
- 6 The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- Usage Monitoring at Flow Level: PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- Usage Monitoring for Static Rules: In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- Usage Monitoring for Predefined Rules: If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
- Usage Monitoring for Dynamic Rules: If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- Usage Monitoring Disabled: If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring

and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.

- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



Important

The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new

usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, see the [Configuring Volume Reporting over Gx](#), on page 386 section.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

3GPP Rel.9 Compliance for IPFilterRule

This section describes the overview and implementation of 3GPP Rel.9 Compliance for IPFilterRule feature.

This section discusses the following topics for this feature:

- [Feature Description](#), on page 416
- [Configuring Rel.9 Compliant AVPs](#), on page 417
- [Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule](#), on page 418

Feature Description

Currently, PCEF is 3GPP Rel. 8 compliant for IPFilterRule in Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs. When PCRF sends the CCA-U or RAR with Flow-Description AVP in Rel. 9 format during a network initiated dedicated bearer creation or modification, PCEF was misinterpreting the source and destination IP address, resulting in sending a wrong TFT to UE.

When the PCRF is upgraded to 3GPP Rel. 9, PCEF still sends CCR-U with Flow-Description, TFT-Filter and Packet-Filter-Content AVPs in Rel. 8 format during UE initiated secondary bearer creation or modification.

To make the PCEF 3GPP Rel. 9 compliant for Flow-Description AVP, TFT-Filter, and Packet-Filter-Content AVPs, the following changes are implemented:

- Interpretation of the source and destination IP address in IPFilterRule in Flow-Description AVP is changed to maintain 3GPP Rel.9 compliancy. That is, when a Rel. 9 Flow-Description for UPLINK is

received during a network-initiated bearer creation or modification, the source IP address is interpreted as remote and the destination as local IP address.

- Traffic flow direction is interpreted from a new Diameter AVP "Flow-Direction". This new AVP indicates the direction or directions that a filter is applicable, downlink only, uplink only or both downlink and uplink (bi-directional).
- IMSA module is modified to encode TFT-Packet-Filter-Information and Packet-Filter-Information AVPs in Rel. 9 format if the negotiated supported feature is Rel. 9 and above.
- Configuration support is provided to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs sent by PCEF in CCR-U. The **diameter 3gpp-r9-flow-direction** CLI command is used to enable Rel. 9 changes. When this CLI command is configured and negotiated supported feature is Rel. 9 or above (both gateway and PCRF are Rel. 9+ compliant), P-GW sends Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

Backward compatibility is maintained, i.e. both Rel. 8 (permit in/out) and Rel. 9 (permit out with flow-direction) formats are accepted by PCEF.

Per the 3GPP Rel. 8 standards, the IPFilterRule in Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs is sent as "permit in" for UPLINK and "permit out" for DOWNLINK direction. From 3GPP Rel. 9 onwards, the Flow-Description AVP within the Flow-Information AVP will have only "permit out" and the traffic flow direction is indicated through Flow-Direction AVP. In 3GPP Rel. 9 format, both UPLINK and DOWNLINK are always sent as "permit out" and hence the usage of "permit in" is deprecated.



Important

This feature is applicable for 3GPP Rel. 9 compliant PCEF and PCRF only when the supported feature negotiated in CCA-I is Rel. 9 or above through the **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.

Relationships to Other Features

This feature works only when the **diameter update-dictionary-avps** CLI command is configured as 3gpp-r9 or 3gpp-r10. That is, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format only when **diameter 3gpp-r9-flow-direction** CLI command is enabled and negotiated supported feature is Rel. 9 or above. The **diameter 3gpp-r9-flow-direction** CLI command for activating this feature must be used only after the PCRF is upgraded to Rel. 9.

Configuring Rel.9 Compliant AVPs

The following section provides the configuration commands to enable Rel.9 changes for Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs.

Encoding AVPs for 3GPP Compliance

Use the following configuration commands to control PCEF from sending Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in Rel. 9 format.

configure

```
context context_name
  ims-auth-service service_name
  policy-control
```

diameter 3gpp-r9-flow-direction
end

- **3gpp-r9-flow-direction**: Encodes Flow-Direction, Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs based on 3GPP Rel. 9 specification. By default, this feature is disabled.
- This CLI configuration is applicable only for TFT-Filter, Packet-Filter-Content, and Flow-Description AVPs sent by PCEF in CCR-U.
- This CLI command must be used only after the PCRF is upgraded to Rel. 9.
- This CLI command works in conjunction with **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }**. When **diameter 3gpp-r9-flow-direction** is configured and negotiated supported feature is 3gpp-r9 or above, PCEF will send Flow-Description, TFT-Filter, and Packet-Filter-Content AVPs in 3GPP Rel. 9 format.

Verifying the Configuration for AVP Compliance

Use the following command to verify the configuration status of this feature.

show ims-authorization service name *service_name*

service_name must be the name of the IMS Authorization service configured for IMS authentication.

The "3GPP R9 Flow Direction Compliance" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name gngp-gx
Context: gngp
IMS Authorization Service name: gngp-gx
Service State: Enabled
Service Mode: Single Interface Policy and Charging
...
Diameter Policy Control:
Endpoint: gx
Origin-Realm: xyz.com
Dictionary: r8-gx-standard
Supported Features:
    3gpp-r9
...
Host Selection: Table: 1 Algorithm: Round-Robin
Host Reselection Subscriber Limit: Not Enabled
Host Reselection Interval: Not Enabled
Sgsn Change Reporting: Not Enabled
3GPP R9 Flow Direction Compliance: Enabled
Host Selection Table[1]: 1 Row(s)
Precedence: 1
...
```

Monitoring and Troubleshooting the 3GPP Rel.9 Compliance for IPFilterRule

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed for any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization service name** *<service_name>* CLI command. If not enabled, configure the **diameter 3gpp-r9-flow-direction** CLI command and check if it works.
- Execute **monitor protocol** command, and check if supported feature negotiated in CCA-I is Rel. 9 or above. If not, this feature will not work. Set the supported feature using **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI command.

- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:
 - monitor protocol log with options 24 (GTPC) and 75-3 (App Specific Diameter - DIAMETER Gx/Ty/Gxx) turned on
 - logs with acsmgr enabled
 - Output of **show active-charging sessions full all** and show ims-authorization sessions CLI commands

show ims-authorization service name

A new field "3GPP R9 Flow Direction Compliance" is added to the output of this show command to indicate whether the Rel. 9 Flow-Direction change is enabled or disabled.

Rel. 10 Gx Interface

Rel. 10 Gx interface support is available on the Cisco ASR chassis running StarOS 15.0 and later releases.

This section describes the following topic:

- [P-GW Rel. 10 Gx Interface Support, on page 419](#)

P-GW Rel. 10 Gx Interface Support

Introduction

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF) on the Packet Data Network (PDN) Gateway (P-GW). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control, or both, by applying AVPs relevant to the application.

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionality. This functional entity is located at the P-GW. The main functions include:

- Control over the user plane traffic handling at the gateway and its QoS.
- Service data flow detection and counting, as well as online and offline charging interactions.
- For a service data flow that is under policy control, the PCEF allows the service data flow to pass through the gateway if and only if the corresponding gate is open.
- For a service data flow that is under charging control, the PCEF allows the service data flow to pass through the gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that charging key.
- If requested by the PCRF, the PCEF will report to the PCRF when the status of the related service data flow changes.

- In case the SDF is tunnelled at the BBERF, the PCEF informs the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

**Important**

ASR 5500 supports only eight flow information including the flow description per dynamic charging rule in a Gx message.

Terminology and Definitions

This section describes features and terminology pertaining to Rel. 10 Gx functionality.

Volume Reporting Over Gx

This section describes the 3GPP Rel. 10 Volume Reporting over Gx feature.

License Requirements

The Volume Reporting over Gx is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

**Important**

In 12.0 and later releases, no separate license is required for Charging over Gx / Volume Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Supported Standards

The Volume Reporting over Gx feature is based on the following standard:

3GPP TS 29.212 V10.5.0 (2012-01): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 10).

Feature Overview

The Volume Reporting over Gx feature provides PCRF the capability to make real-time decisions based on the data usage by subscribers.

**Important**

Volume Reporting over Gx is applicable only for volume quota.

In release 10.0, only total data usage reporting is supported, uplink/downlink level reporting is not supported. In 10.2 and later releases, it is supported.

The PCEF only reports the accumulated usage since the last report for usage monitoring and not from the beginning.

If the usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

In 12.2 and later releases, usage reporting on bearer termination is supported.

The following steps explain how Volume Reporting over Gx works:

- 1 PCEF after receiving the message from PCRF parses the usage monitoring related AVPs, and sends the information to IMSA.
- 2 IMSA updates the information to ECS.
- 3 Once the ECS is updated with the usage monitoring information from PCRF, the PCEF (ECS) starts tracking the data usage.
- 4 For session-level monitoring, the ECS maintains the amount of data usage.
- 5 For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the usage information per monitoring key. When the data traffic is passed, the usage is checked against the usage threshold values and reported as described in the *Usage Reporting* section.
- 6 The PCEF continues to track data usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session.

Usage Monitoring

- Usage Monitoring at Session Level: PCRF subscribes to the session-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL(0). After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. In 11.0 and later releases, Monitoring Key at session level is supported.

In 12.0 and later releases, enabling and disabling session usage in a single message from PCRF is supported. This is supported only if the monitoring key is associated at session level.

In 12.0 and later releases, monitoring of usage based on input/output octet threshold levels is supported. Usage is reported based on the enabled threshold level. If multiple levels are enabled, usage will be reported on all the enabled levels even if only one of the levels is breached. Monitoring will be stopped on the missing threshold levels in the response for the usage report from PCRF (expected to provide the complete set again if PCRF wants to continue monitoring on the multiple levels enabled earlier).

Total threshold level along with UL/DL threshold level in the GSU AVP is treated as an error and only total threshold level is accepted.

In releases prior to 17.0, extra CCR-U was generated for a monitoring key when the following requests are received in the response to the CCR-U which reported the usage for the same monitoring key.

- immediate reporting request with monitoring key at rule level
- immediate reporting request with or without monitoring key at session level
- explicit disable request at rule level
- explicit disable request at session level

In 17.0 and later releases, extra CCR-U is not generated for a monitoring key when all the above mentioned requests are received in the response to the CCR-U which reported the usage for the same monitoring key. Also, extra CCR-U is not generated when immediate reporting request without monitoring key at rule level is received in the response to the CCR-U which reported the usage for all the active monitoring keys.

- **Usage Monitoring at Flow Level:** PCRF subscribes to the flow-level volume reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow-level monitoring since the rules are associated with the monitoring key and enabling/disabling of usage monitoring at flow level can be controlled by PCRF using it. After the AVPs are parsed by DPCA, IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.

Usage monitoring is supported for static, predefined rules, and dynamic rule definitions.

- **Usage Monitoring for Static Rules:** In the case of static rules, the usage reporting on last rule removal associated with the monitoring key is not applicable. In this case only the usage monitoring information is received from the PCRF.
- **Usage Monitoring for Predefined Rules:** If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The Monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the data being tracked for multiple rules having the same monitoring key. After DPCA parses the AVPs IMSA updates the information to ECS. Once ECS is updated usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present.
- **Usage Monitoring for Dynamic Rules:** If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This would result in the usage monitoring being done for all the rules associated with that monitoring key. After DPCA parses the AVPs, IMSA updates the information to ECS. Once ECS is updated, the usage monitoring is started and constantly checked with the usage threshold whenever the data traffic is present. Monitoring key for dynamic ruledef is dynamically assigned by PCRF which is the only difference with predefined rules in case of usage monitoring.

In releases prior to 15.0, when threshold breach happens for multiple monitoring keys at the same time, only one of the monitoring keys' usage is reported and the rest of the monitoring keys' usage is reported in CCR-T (threshold set to infinity). On Tx expiry/TCP link error, unreported usage is stored at ECS and reported only on session termination.

In 15.0 and later releases, only one of the monitoring keys' usage is reported first. Upon receiving successful response from PCRF, the rest of the monitoring keys' usage is reported to PCRF. On Tx expiry/TCP link error, unreported usage is stored at ECS. Any future successful interaction with PCRF for the session will send unreported UMI to PCRF.

Usage Reporting

Usage at subscriber/flow level is reported to PCRF under the following conditions:

- **Usage Threshold Reached:** PCEF records the subscriber data usage and checks if the usage threshold provided by PCRF is reached. This is done for both session and rule level reporting.

For session-level reporting, the actual usage volume is compared with the usage volume threshold.

For rule-level reporting the rule that hits the data traffic is used to find out if the monitoring key is associated with it, and based on the monitoring key the data usage is checked. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by the PCRF. The Usage-Monitoring-Information AVP is sent in this CCR with the "Used-Service-Unit" set to the amount of data usage by subscriber.

If PCRF does not provide a new usage threshold in the usage monitoring information as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no usage status is reported.

In the non-standard Volume Reporting over Gx implementation, usage monitoring will be stopped once the threshold is breached, else the monitoring will continue. There will be no further usage reporting until the CCA is received.

- **Usage Monitoring Disabled:** If the PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, the PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger. If the PCRF does not provide a new usage threshold as a result of CCR from PCEF when the usage threshold is reached, the usage monitoring is stopped at PCEF and no further usage status is reported.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF. If PCC usage level information is enabled by PCRF, the PCC usage will also be reported.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, the PCEF sends a CCR with the data usage for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key. In 12.0 and later releases, usage reporting on last rule deactivation using rule deactivation time set by PCRF is supported.

Releases prior to 14.0, when PCC rule was tried to be removed while waiting for access side update bearer response, the charging rules were not removed. In 14.0 and later releases, on receiving message from PCRF, the rule that is meant for removal is marked and then after the access side procedure is complete the rule is removed.

- **PCRF Requested Usage Report:** In 10.2 and later releases, the accumulated usage since the last report is sent even in case of immediate reporting, the usage is reset after immediate reporting and usage monitoring continued so that the subsequent usage report will have the usage since the current report. In earlier releases the behavior was to accumulate the so far usage in the next report.
- **Release 12.2 onwards,** usage reporting on bearer termination can be added. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.
- **Revalidation Timeout:** In the non-standard implementation, if usage monitoring and reporting is enabled and a revalidation timeout occurs, the PCEF sends a CCR to request PCC rules and reports all accumulated usage for all enabled monitoring keys since the last report (or since usage reporting was enabled if the usage was not yet reported) with the accumulated usage at IP-CAN session level (if enabled) and at service data flow level (if enabled) This is the default behavior.

In the case of standard implementation, this must be enabled by CLI configuration.



Important

The Usage Reporting on Revalidation Timeout feature is available by default in non-standard implementation of Volume Reporting over Gx. In 10.2 and later releases, this is configurable in the standard implementation. This is not supported in 10.0 release for standard based volume reporting.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track data usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then usage monitoring does not continue in the PCEF for that IP CAN session and the usage accumulated between the CCR-CCA will be discarded.

In releases prior to 17.0, CCR-U triggered on server retries does not take server granted quota into account for reporting USU. In 17.0 and later releases, CCR-U triggered on server retries takes server granted quota into account for reporting USU. For newly created MSCC, interim quota configuration is taken as reference for reporting USU.

For information on how to configure the Volume Reporting over Gx feature, refer to [Configuring Volume Reporting over Gx](#), on page 386.

ICSR Support for Volume Reporting over Gx (VoRoGx)

In releases prior to 15.0, post the ICSR switchover, any existing session for which the PCRF has enabled volume reporting used to continue indefinitely until the session is terminated or until CCR-U is sent for a given trigger, without having the volume counted via Gx.

To summarize, after an ICSR switchover, volume reporting over Gx is no longer done for existing sessions. Also, volume usage is not synced to standby chassis.

In 15.0 and later releases, volume threshold and volume usage are synced to standby chassis to support volume reporting over Gx for existing sessions post switchover.

Without this support it cannot cause a subscriber to use higher speeds than what s/he is supposed to get, if volume reporting is for example used to enforce fair usage; the operator may already consider this a revenue loss. It will also severely impact roaming subscribers who are supposed to get a notification and be blocked/redirected once the limits set by the EU roaming regulation are reached. If a session continues now without being blocked, the operator is not allowed to charge for data beyond the limit and will have a significant and real revenue loss (roaming partner may still charge for the data used on their SGSNs).

Use of the Supported-Features AVP on the Gx Interface

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client will, in the first request in a Diameter session indicate the set of features required for the successful processing of the session. If there are features supported by the client that are not advertised as part of the required set of features, the client will provide in the same request this set of optional features that are optional for the successful processing of the session. The server will, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server will support within the same Diameter session. Any further command messages will always be compliant with the list of supported features indicated in the Supported-Features AVPs and features that are not indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported will not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the Gx reference point

will be compliant with the requirements for dynamic discovery of supported features and associated error handling.

The base functionality for the Gx reference point is the 3GPP Rel. 7 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the Gx commands. As defined in 3GPP TS 29.229, when extending the application by adding new AVPs for a feature, the new AVPs will have the M bit cleared and the AVP will not be defined mandatory in the command ABNF.

The Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the Gx reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, the Vendor-Id AVP will contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the Gx reference point, the Feature-List-ID AVP will differentiate those lists from one another.

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits.
1	Rel9	M	This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.
3	Rel10	M	This feature indicates the support of base 3GPP Rel-10 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits.
4	SponsoredConnectivity	O	This feature indicates support for sponsored data connectivity feature. If the PCEF supports this feature, the PCRF may authorize sponsored data connectivity to the subscriber.

In releases prior to 15.0, the Supported-Features AVP was not encoded in CCR-U messages, but it was supported only in CCR-I message. If Rel. 8 dictionary or any dictionary beyond Rel. 8 is used and PCRF does not provide Supported-Features AVP in CCA-I, then the call gets dropped.

In 15.0 and later releases, if PCEF configures Diameter dictionary as release 8, 9 or 10, then PCRF sends Supported-Features AVP so that PCEF will know what feature PCRF supports. If PCEF receives supported features lesser than or greater than requested features then supported feature will be mapped to the lower one.

Whenever the custom dictionary "dpca-custom24" is configured, the Supported-Features AVP including Vendor-Id AVP will be sent in all CCR messages.

Rule-Failure-Code AVP

The Rule-Failure-Code AVP indicates the reason that the QoS/PCC rules cannot be successfully installed/activated or enforced. The Rule-Failure-Code AVP is of type Enumerated. It is sent by the PCEF to the PCRF within a Charging-Rule-Report AVP to identify the reason a PCC Rule is being reported.

In releases prior to 15.0, only 11 rule failure codes were defined as the values for this AVP. In 15.0 and later releases, two new rule failure codes `INCORRECT_FLOW_INFORMATION` (12) and `NO_BEARER_BOUND` (15) are added. The name of the existing rule failure code 9 is changed to `MISSING_FLOW_INFORMATION`. For 3GPP Rel. 10, rule failure code 9 maps to `GW/PCEF_MALFUNCTION`.

Sponsored Data Connectivity

With Sponsored Data Connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

Sponsored Data Connectivity feature is introduced in Rel. 10 of 3GPP TS 29.212 specification. If Sponsored Data Connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) who is willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level `"SPONSORED_CONNECTIVITY_LEVEL"` is added for reporting at Sponsor Connection level and two new AVPs `"Sponsor-Identity"` and `"Application-Service-Provider-Identity"` have been introduced at the rule level.

Sponsored Data Connectivity will be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the Application Function (AF).

The provisioning of sponsored data connectivity per PCC rule will be performed using the PCC rule provisioning procedure. The sponsor identity will be set using the Sponsor-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. The application service provider identity will be set using the Application-Service-Provider-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. Sponsor-Identity AVP and Application-Service-Provider-Identity AVP will be included if the Reporting-Level AVP is set to the value `SPONSORED_CONNECTIVITY_LEVEL`.

When receiving the flow based usage thresholds from the AF, the PCRF will use the sponsor identity to generate a monitoring key. The PCRF may also request usage monitoring control, in this case, only the flow based usage is applied for the sponsored data connectivity. If requested, the PCEF may also report the usage to the PCRF.

A new CLI command **"diameter encode-supported-features"** has been added in Policy Control Configuration mode to send supported features with Sponsor Identity. For more information on the command, see the *Command Line Interface Reference*.

Sponsored connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also sponsored connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature will be turned off.

This feature implementation impacts only the Gx dictionary `"dpca-custom15"`. Also note that this feature is supported only for the dynamic rules.

Volume Reporting

For Volume Reporting over Gx, PCRF generates a unique monitoring key based on sponsor identity. Since flows with different monitoring keys are treated differently, flows with sponsor ID are charged differently.

Supported Gx Features

Assume Positive for Gx

In a scenario where both the primary and secondary PCRF servers are overloaded, the PCRF returns an error to P-GW and HSGW. Current behavior for the P-GW and HSGW is to terminate the session if both primary and secondary return a failure or timeout.

This feature is developed to enhance this behavior by applying local policy on the GW to ensure that the subscriber session continues. P-GW / HSGW should implement Assume Positive feature to handle errors and based on the event type implement specific rules.



Important

Use of Gx Assume Positive requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

The failure handling behavior is enhanced to ensure that the subscriber service is maintained in case of PCRF unavailability. It is also required that the GW reduces the traffic towards the PCRF when receiving a Diameter Too Busy (3004) by stopping the transmission and reception of Diameter messages (CCRs and RARs) to and from the PCRF for a configurable amount of time.

In case of any of the following failures with PCRF, the GW chooses to apply failure handling which results in subscriber termination or to allow browsing without any more policy enforcement.

- TCP link failure
- Application Timer (Tx) expiry
- Result code based failures

In 14.1 and later releases, the PCRF is allowed to fall back to Local Policy for all connection level failures, result code/experimental result code failures. Local Policy may choose to allow the subscriber for a configured amount of time. During this time any subscriber/internal event on the call would be handled from Local Policy. After the expiry of the timer, the subscriber session can be either terminated or else PCRF can be retried. Note that the retry attempt to PCRF happens only when the **timer-expiry event** is configured as **reconnect-to-server**.

The fallback support is added to the failure handling template and the local policy service needs to be associated to IMS Authorization service.

Once the local policy is applied, all PCRF enabled event triggers will be disabled. When the subscriber session is with the local-policy, the GW skips sending of CCR-T and cleans up the session locally.

For a session that was created with active Gx session, the GW sends the CCR-T to primary and on failure sends the CCR-T to the secondary PCRF. If the CCR-T returns a failure from both primary and secondary or times out, the GW cleans up the session locally.

Fallback to Local Policy is done in the following scenarios:

- Tx timer expiry

- Diabase Error
- Result Code Error (Permanent/Transient)
- Experimental Result Code
- Response Timeout

The following points are applicable only in the scenario where reconnect to PCRF is attempted.

- If the subscriber falls back to local-policy because of CCR-I failure, CCR-I will be sent to the PCRF after the timer expiry. On successful CCA-I call will be continued with PCRF or else the call will be continued with local-policy and retry-count will be incremented.
- If the subscriber falls back to local-policy because of the CCR-U failure, IMS Authorization application waits for some event change to happen or to receive an RAR from PCRF.
- In case of event change after the timer expiry, CCR-U will be sent to PCRF. On successful CCA-U message, call will be continued with PCRF or else call will be with local-policy and retry-count will be incremented.
- If RAR is received after the timer-expiry the call will be continued with the PCRF. On expiry of maximum of retries to connect to PCRF, call will be disconnected.

Default Policy on CCR-I Failure

The following parameters are supported for local configuration on P-GW. The configuration parameters are configurable per APN and per RAT Type.

The following fields for a Default Bearer Charging Rule are configurable per APN and per RAT Type:

- Rule Name
- Rating Group
- Service ID
- Online Charging
- Offline Charging
- QCI
- ARP
 - Priority Level
 - QCI
 - QVI
- Max-Requested-Bandwidth
 - UL
 - DL

Flow Description and Flow Status are not configurable but the default value will be set to Any to Any and Flow Status will be set to Enabled.

The following command level fields are configurable per APN and per RAT Type:

- AMBR
 - UL
 - DL
- QCI
- ARP
 - Priority Level
 - QCI
 - QVI

Gx Back off Functionality

This scenario is applicable when Primary PCRF cluster is unavailable but the secondary PCRF is available to handle new CCR-I messages.

When the chassis receives 3004 result-code then back-off timer will be started for the peer and when the timer is running no messages will be sent to that peer.

The timer will be started only when the value is being configured under endpoint configuration.

Releases prior to 15.0, when the IP CAN session falls back to local policy it remained with local policy until the termination timer expires or the subscriber disconnects. Also, the RAR message received when the local-policy timer was running got rejected with the cause "Unknown Session ID".

In 15.0 and later releases, P-GW/GGSN provides a fair chance for the subscriber to reconnect with PCRF in the event of CCR failure. To support this feature, configurable validity and peer backoff timers are introduced in the Local Policy Service and Diameter endpoint configuration commands. Also, the RAR received when the local-policy timer is running will be rejected with the cause "DIAMETER_UNABLE_TO_DELIVER".

In releases prior to 17.0, rule report was not sent in the CCR messages when PCRF is retried after the expiry of validity timer. In 17.0 and later releases, rule report will be sent to the PCRF during reconnect when the CLI command **diameter encodeevent-avps local-fallback** is configured under Policy Control Configuration mode.

Support for Volume Reporting in Local Policy

This feature provides support for time based reconnect to PCRF instead of the event based for CCR-U failure scenarios.

In releases prior to 17.0, the following behaviors were observed with respect to the Volume Reporting for Local Policy:

- In the event of CCR-U failure, CCR-U was triggered to PCRF only on receiving subscriber event.
- When a CCR-U failure happened and a call continued without Gx, unreported volume is lost as the threshold is set to infinity. In next CCR-U triggered to PCRF, the cumulative volume was sent to PCRF.
- RAR was rejected with result-code `diameter_unable_to_comply` (3002) when the validity timer is running.

In 17.0 and later releases, with the timer-based implementation, this feature introduces the following changes to the existing behavior:

- When send-usage-report is configured, the CCR-U with usage report will be sent immediately after the local-policy timer-expiry.
- The unreported usage will not be returned to ECS. Thus, usage since last tried CCR-U will be sent to PCRF.
- RAR will be accepted and the rules received on RAR will be installed even when the timer is running.

Session can be connected to PCRF immediately instead of waiting for subscriber event, and the updated usage report can be sent.

Support for Session Recovery and Session Synchronization

Currently PCRF and ASR 5500 gateway node are in sync during normal scenarios and when Gx assume positive is not applied. However, there are potential scenarios where the PCRF might have been locally deleted or lost the Gx session information and it is also possible that due to the loss of message, gateway node and PCRF can be out of sync on the session state.

While these are rare conditions in the network, the desired behavior is to have PCRF recover the Gx session when it is lost and also to have PCRF and gateway sync the rule and session information. This feature provides functionality to ensure PCRF and gateway can sync on session information and recover any lost Gx sessions. Configuration support has been provided to enable session recovery and session sync features.

In releases prior to 17.0, the implementation is as follows:

- If the PCRF deletes or loses session information during a Gx session update (CCR-U) initiated by the gateway, PCRF will respond back with DIAMETER_UNKNOWN_SESSION_ID resulting in session termination even in the case of CCR-U.
- If the PCRF deletes or loses session information and an Rx message is received, PCRF will not be able to implement corresponding rules and will result in failure of subscriber voice or video calls.
- For subscriber's existing Rx sessions and active voice/video calls, PCRF will not be able to initiate cleanup of the sessions towards the gateway and can result in wastage of the resources in the network (dedicated bearers not removed) or can result in subscriber not able to place calls on hold or conference or remove calls from hold.
- For out of sync scenarios, PCRF and gateway could be implementing different policies and can result in wastage of resources or in poor subscriber experience. Existing behavior does not provide for a way to sync the entire session information.

In 17.0 and later releases, the gateway (GW) node and PCRF now supports the ability to exchange session information and the GW provides the complete subscriber session information to enable PCRF to build the session state. This will prevent the occurrence of the above mentioned scenarios and ensure that GW and PCRF are always in sync. The keywords **session-recovery** and **session-sync** are used with the **diameter encode-supported-features** CLI command in Policy Control Configuration mode to support Gx Synchronization.

Configuring Gx Assume Positive Feature

To configure Gx Assume Positive functionality:

-
- Step 1** At the global configuration level, configure Local Policy service for subscribers as described in the [Configuring Local Policy Service at Global Configuration Level](#), on page 431.
- Step 2** At the global configuration level, configure the failure handling template to use the Local Policy service as described in the [Configuring Failure Handling Template at Global Configuration Level](#), on page 432.
- Step 3** Within the IMS Authorization service, associate local policy service and failure handling template as described in the [Associating Local Policy Service and Failure Handling Template](#), on page 432.
- Step 4** Verify your configuration as described in the [Verifying Local Policy Service Configuration](#), on page 432.
- Step 5** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Important** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.
-

Configuring Local Policy Service at Global Configuration Level

Use the following example to configure Local Policy Service at global configuration level for subscribers:

```
configure
local-policy-service LOCAL_PCC
    ruledef 2G_RULE
        condition priority 1 apn match .*
        exit
    ruledef all-plmn
        condition priority 1 serving-plmn match .*
        exit
    actiondef 2G_UPDATE
        action priority 1 activate-ambr uplink 18000 downlink 18000
        action priority 2 reject-requested-qos
        exit
    actiondef action1
        action priority 2 allow-requested-qos
        exit
    actiondef allow
        action priority 1 allow-session
        exit
    actiondef delete
        action priority 1 terminate-session
        exit
    actiondef lp_fall
        action priority 1 reconnect-to-server
        exit
    actiondef time
```

```

    action priority 1 start-timer timer duration 10
exit
eventbase default
    rule priority 1 event fallback ruledef 2G_RULE actiondef time continue
    rule priority 2 event new-call ruledef 2G_RULE actiondef action1
    rule priority 3 event location-change ruledef 2G_RULE actiondef action1
    rule priority 5 event timer-expiry ruledef 2G_RULE actiondef lp_fall
    rule priority 6 event request-qos default-qos-change ruledef 2G_RULE actiondef allow
end

```

Notes:

- On occurrence of some event, event will be first matched based on the priority under the eventbase default. For the matched rule and if the corresponding ruledef satisfies, then specific action will be taken.

Configuring Failure Handling Template at Global Configuration Level

Use the following example to configure failure handling template at global configuration level:

```

configure
failure-handling-template <template_name>
msg-type any failure-type any action continue local-fallback
end

```

Notes:

- When the TCP link failure, Application Timer (Tx) expiry, or Result code based failure happens, the associated failure-handling will be considered and if the failure-handling action is configured as local-fallback, then call will fall back to local-fallback mode.

Associating Local Policy Service and Failure Handling Template

Use the following example to associate local policy service and failure handling template:

```

configure
context <context_name>
ims-auth-service <service_name>
    associate local-policy-service <lp_service_name>
    associate failure-handling <failure-handling-template-name>
end

```

Verifying Local Policy Service Configuration

To verify the local policy service configuration, use this command:

```
show local-policy statistics service service_name
```

Time Reporting Over Gx

This section describes the Time Reporting over Gx feature supported for GGSN in this release.

License Requirements

No separate license is required for Time Reporting over Gx feature. This feature can be enabled as part of "Policy Interface" license.

Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Feature Overview

This non-standard Time Usage Reporting over Gx feature is similar to Volume Usage Reporting over Gx. PCRF provides the time usage threshold for entire session or particular monitoring key in CCA or RAR. When the given threshold breached usage report will be sent to PCRF in CCR. This time threshold is independent of data traffic. Apart from the usage threshold breach there are other scenarios where usage report will be send to PCRF.



Important

Time reporting over Gx is applicable only for time quota.

The PCEF only reports the accumulated time usage since the last report for time monitoring and not from the beginning.

If the time usage threshold is set to zero (infinite threshold), no further threshold events will be generated by PCEF, but monitoring of usage will continue and be reported at the end of the session.

Time usage reporting on bearer termination is supported. When a bearer is deleted due to some reason, the rules associated with the bearer will also be removed. So, the usage will be reported on the monitoring key(s) whose associated rule is the last one that is removed because of bearer termination.

The following steps explain how Time Reporting over Gx works:

- 1 PCEF after receiving the message from PCRF parses the time monitoring related AVPs, and sends the information to IMSA.
- 2 IMSA updates the information to ECS.
- 3 Once the ECS is updated with the time monitoring information from PCRF, the PCEF (ECS) starts tracking the time usage.
- 4 For session-level monitoring, the ECS maintains the amount of time usage.
- 5 For PCC rule monitoring, usage is monitored with the monitoring key as the unique identifier. Each node maintains the time usage information per monitoring key.
- 6 The PCEF continues to track time usage after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time monitoring does not continue in the PCEF for that IP CAN session.

Limitations

This section lists the limitations for Time Reporting over Gx in this release.

- Only integer monitoring key will be supported like Volume Reporting over Gx
- If the same monitoring key is used for both time and data volume monitoring then disabling monitoring key will disable both time and data usage monitoring.
- If the same monitoring key is used for both time and data usage monitoring and if an immediate report request is received, then both time and volume report of that monitoring key will be sent.

Usage Monitoring

Two levels of time usage reporting are supported:

- Usage Monitoring at Session Level
- Usage Monitoring at Flow Level

Usage Monitoring at Session Level

PCRF subscribes to the session level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to SESSION_LEVEL (0).

Usage Monitoring at Flow Level

PCRF subscribes to the flow level time reporting over Gx by sending the Usage-Monitoring-Information AVP with the usage threshold level set in Granted-Service-Unit AVP and Usage-Monitoring-Level AVP set to PCC_RULE_LEVEL(1). Monitoring Key is mandatory in case of a flow level monitoring since the rules are associated with the monitoring key and enabling or disabling of usage monitoring at flow level can be controlled by PCRF using it. Usage monitoring is supported for both predefined rules and dynamic rule definition.

Usage Monitoring for Predefined and Static Rules

If the usage monitoring needs to be enabled for the predefined rules, PCRF sends the rule and the usage monitoring information containing the monitoring key and the usage threshold. The monitoring key should be same as the one pre-configured in PCEF for that predefined rule. There can be multiple rules associated with the same monitoring key. Hence enabling a particular monitoring key would result in the time being tracked for multiple rules having the same monitoring key. Similarly, usage monitoring information is sent from PCRF for the static rules also.

Usage Monitoring for Dynamic Ruledefs

If the usage monitoring needs to be enabled for dynamic ruledefs, PCRF provides the monitoring key along with a charging rule definition and the usage monitoring information containing the monitoring key and the usage threshold. This results in the usage monitoring being done for all the rules associated with that monitoring key.

Usage Reporting

Time usage at subscriber/flow level is reported to PCRF under the following conditions:

- Usage Threshold Reached: PCEF records the subscriber usage and checks if the usage threshold provided by PCRF is reached. Once the condition is met, it reports the usage information to IMSA and continues monitoring. IMSA then triggers the CCR-U if "USAGE_REPORT" trigger is enabled by PCRF. The

Usage-Monitoring-Information AVP is sent in this CCR with the "CC-Time" in "Used-Service-Unit" set to track the time usage of the subscriber.

- **Usage Monitoring Disabled:** If PCRF explicitly disables the usage monitoring with Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED, PCEF stops monitoring and reports the usage information (when the monitoring was enabled) to PCRF if the usage monitoring is disabled by PCRF as a result of CCR from PCEF which is not related to reporting usage, other external triggers, or a PCRF internal trigger.
- **IP CAN Session Termination:** When the IP CAN session is terminated, the accumulated subscriber usage information is reported to PCRF in the CCR-T from PCEF.

PCRF uses RAR message and includes Session-Release-Cause AVP in it to initiate IP CAN Session Termination. However, there are some scenarios where PCRF may want to terminate the IP CAN Session in CCA messages. In order to avoid an unnecessary additional message, PCRF can inform P-GW to terminate the subscriber in CCA-U message itself. Hence, in 17.0 and later releases, the Session Release Cause has been added in CCA messages for all Gx dictionaries.

- **PCC Rule Removal:** When the PCRF deactivates the last PCC rule associated with a usage monitoring key, PCEF sends a CCR with the usage time for that monitoring key. If the PCEF reports the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key.
- **PCRF Requested Usage Report:** When PCRF provides the Usage-Monitoring-Information with the Usage-Monitoring-Report set to USAGE_MONITORING_REPORT_REQUIRED, PCEF sends the time usage information. If the monitoring key is provided by PCRF, time usage for that monitoring key is notified to PCRF regardless of usage threshold. If the monitoring key is not provided by PCRF, time usage for all enabled monitoring keys is notified to PCRF.
- **Event Based Reporting:** The event based reporting can be enabled through the CLI command **event-update send-usage-report events**. When an event like sgsn change, qos change or revalidation-timeout is configured under this CLI, time usage report is generated whenever that event happens.

Once the usage is reported, the usage counter is reset to zero. The PCEF continues to track time usage from the zero value after the threshold is reached and before a new threshold is provided by the PCRF. If a new usage threshold is not provided by the PCRF in the acknowledgement of an IP-CAN Session modification where its usage was reported, then time usage monitoring does not continue in the PCEF for that IP CAN session.

For information on how to configure the Time Reporting over Gx feature, see the [Configuring Time Reporting over Gx](#), on page 435.

Configuring Time Reporting over Gx

This section describes the configuration required to enable Time Reporting over Gx.

To enable Time Reporting over Gx, use the following configuration:

configure

active-charging service <ecs_service_name>

rulebase <rulebase_name>

action priority <priority> **dynamic-only ruledef** <ruledef_name> **charging-action** <charging_action_name> **monitoring-key** <monitoring_key>

```

    exit
  exit
context <context_name>
  ims-auth-service <imsa_service_name>
  policy-control
    event-update send-usage-report [ reset-usage ]
  end
end

```

Notes:

- The configuration for enabling Time Reporting over Gx is same as the Volume Reporting over Gx configuration. If a time threshold is received from PCRF then Time monitoring is done, and if a volume threshold is received then Volume monitoring will be done.
- The maximum accepted monitoring key value by the PCEF is 4294967295. If the PCEF sends a greater value, the value is converted to an Unsigned Integer value.
- The **event-update** CLI enables time usage report to be sent in event updates. The optional keyword **reset-usage** enables to support delta reporting wherein the usage is reported and reset at PCEF. If this option is not configured, the behavior is to send the time usage information as part of event update but not reset at PCEF.

Support for Multiple Active and Standby Gx Interfaces to PCRF

In the earlier Gx implementation, Diameter Policy Control Application has the limitation to mandatorily configure hosts as part of IMS Authorization service or associate a host template and select the hosts to be communicated for each subscriber session. Since the peer selection can happen at diabase and application need not select any hosts, this feature is developed to remove the restrictions imposed in the application and allow diabase to pick the peers in a round robin fashion. In addition, this feature will take care of peer selection at diabase even when the hosts picked by application are not active. This change in behavior is controlled through the CLI command "**endpoint-peer-select**" as the default behavior is to drop the call if the server discovery fails at application.

When the call is established, IMSA module checks the host selection table/prefix table/host template associated in IMSA service to pick the primary and secondary peers to be contacted. If no host table/prefix table/host template is configured or none of the rows in prefix table are matching or the hosts selected by IMSA are inactive, then based on the CLI configuration the control is given to diabase module which will select the peers in a round robin fashion or terminate the call based on the CLI configuration.

When the CCR message results in a diabase error/Tx expiry/response timeout, then IMSA will let diabase select an alternate route by excluding the peer which resulted in the failure and switch to the peer if the lookup is successful.

When CCR/CCA message is exchanged with the directly connected host selected by diabase and RAR message is received from new host, then IMSA will skip host configuration check and let further communication to happen with the new host. If the directly connected host is selected by application during call establishment, then IMSA will check if the new host is the secondary server per application. When the CCR/CCA message is exchanged with indirectly connected host through DRA which is picked by diabase and RAR message is received from same host through another DRA, then IMSA will skip host configuration check and let further communication to happen with the same host through the new DRA. If the DRA is selected by application during call establishment, then IMSA will check if the new DRA is the secondary server per application. Even if RAR message is received from different host though another DRA, IMSA will skip host configuration check and let further communication to happen with the new host through the new DRA.

Configuring Diameter Peer Selection at Diabase in Failure Scenarios

The following configuration enables diabase to select the Diameter peers when IMSA fails.

```
configure
context context_name
ims-auth-service service_name
policy-control
  endpoint-peer-select [ on-host-select-failure | on-inactive-host ]
  { default | no } endpoint-peer-select
end
```

Notes:

- This command is used to perform server selection at diabase when the hosts could not be selected by IMS Authorization application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts.
- **on-host-select-failure**: Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.
- **on-inactive-host**: Specifies to perform server selection at diabase when the hosts selected by application are inactive.
- This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at IMS Authorization application.

Support for Multiple CCR-U's over Gx Interface

ASR 5500 node earlier supported only one pending CCR-U message per session over Gx interface. Any request to trigger CCR-U (for access side updates/internal updates) were ignored/dropped, when there was already an outstanding message pending at the node. PCEF and PCRF were out of synch if CCR-U for critical update was dropped (like RAT change/ULI change).

In 17.0 and later releases, ASR 5500 supports multiple CCR-U messages at a time per session through the use of a configurable CLI command "**max-outstanding-ccr-u**" under IMS Authorization Service configuration mode. That is, this CLI will allow the user to configure a value of up to 12 as the maximum number of CCR-U messages per session.

The CLI-based implementation allows sending request messages as and when they are triggered and processing the response when they are received. The gateway does re-ordering if the response messages are received out of sequence.

To support multiple outstanding messages towards PCRF, the following items should be supported:

- Allowing IMSA to send multiple CCR-U messages – This can be achieved through the use of **max-outstanding-ccr-u** command in the IMS Authorization Service configuration mode.
- Queuing of response message for ordering – DPCA should parse the received message irrespective of order in which they are received. IMSA will check whether to forward the response to session manager or queue it locally.

- Peer switch – When multiple CCR-Us are triggered, IMSA will start Tx timer for each request sent out. On first Tx expiry, IMSA/DPCA will do peer switch. That is, IMSA will stop all other requests' Tx timers and switch to secondary peer (if available) or take appropriate failure handling action.
- Failure handling – On peer switch failure due to Tx expiry, DPCA will take failure handling action based on the configuration present under ims-auth-service.
- Handling back pressure – In case of multiple CCR-Us triggered to Primary PCRF and due to Tx timeout all the messages are switched to Secondary PCRF. If Secondary server is already in backpressure state, then IMSA will put first message in the backpressure queue and once after message is processed next pending request will be put into BP queue.
- Volume reporting – In case of multiple CCR-Us for usage report is triggered (for different monitoring keys) and failure handling is configured as "**continue send-ccrt-on-call-termination**", on first Tx timeout or response timeout, usage report present in all the CCR-Us will be sent to ECS. All the unreported usage will be sent in CCR-T message when the subscriber goes down. If "**event-update send-usage-report**" CLI is present, then there are chances of reporting usage for same monitoring key in multiple CCR-Us.

Though the **max-outstanding-ccr-u** CLI command supports configuring more than one CCR-U, only one outstanding CCR-U for access side update is sent out at a time and multiple CCR-Us for internal updates are sent.

These are the access side updates for which CCR-U might be triggered:

- Bearer Resource Command
- Modify Bearer Request (S-GW change, RAT change, ULI change)
- Modify Bearer Command

These are the following internal updates for which CCR-U is triggered:

- S-GW restoration
- Bearer going down (GGSN, BCM UE_Only)
- ULI/Timezone notification
- Default EPS bearer QoS failure
- APN AMBR failure
- Charging-Rule-Report
- Out of credit / reallocation of credit
- Usage reporting
- Tethering flow detection
- Access network charging identifier

Configuring Gateway Node to Support Back-to-Back CCR-Us

The following configuration enables or disables the gateway to send multiple back-to-back CCR-Us to PCRF.

```
configure
context context_name
```

```

ims-auth-service service_name
  policy-control
    [ default ] max-outstanding-ccr-u value
  end

```

Notes:

- *value* must be an integer value from 1 through 12. The default value is 1.

Support for RAN/NAS Cause IE on Gx Interface

New supported feature "Netloc-RAN-NAS-Cause" has been introduced to be in compliance with the Release 12 specification of 3GPP TS 29.212. This feature is used to send detailed RAN and/or NAS release cause code information from the access network to PCRF. It requires that the NetLoc feature is also supported.



Important

This feature can be enabled only when the NetLoc feature license is installed.

A new Diameter AVP "RAN-NAS-Release-Cause" will be included in the Charging-Rule-Report AVP and in CCR-T for bearer and session deletion events respectively, when the NetLoc-RAN-NAS-Cause supported feature is enabled. This AVP will indicate the cause code for the subscriber/bearer termination.

Configuring Supported Feature Netloc-RAN-NAS-Cause

The following configuration enables the supported feature "Netloc-RAN-NAS-Cause".

```

configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features netloc-ran-nas-cause
      end
    end
  end

```

Notes:

- **netloc-ran-nas-cause:** Enables the Netloc-RAN-NAS-Cause feature. By default, this supported feature will be disabled.
- If the supported features "netloc-ran-nas-code" and "netloc" are enabled, then netloc-ran-nas-cause code will be sent to PCRF.

To disable this supported feature, use the following command:

```
[ default | no ] diameter encode-supported-features
```

Support ADC Rules over Gx Interface

In this release, P-GW will use Application Detection and Control (ADC) functionality over Gx as defined in the Release 11 specification of 3GPP standard.

ADC extension over Gx provides the functionality to notify PCRF about the start and stop of a specific protocol or a group of protocols, and provide the possibility to PCRF that with the knowledge of this information, change the QoS of the user when the usage of application is started and until it is finished.

The provision of ADC information is done through the ADC rule, the action initiated by PCRF is done through the PCC rule.

ADC rules are certain extensions to dynamic and predefined PCC rules in order to support specification, detection and reporting of an application flow. These rules are installed (modified/removed) by PCRF via CCA-I/CCA-U/RAR events. ADC rules can be either dynamic PCC or predefined PCC rules, and the existing attributes of dynamic and predefined rules will be applicable.

Dynamic PCC rule contains either traffic flow filters or Application ID. When Application ID is present, the rule is treated as ADC rule. Application ID is the name of the ruledef which is pre-defined in the boxer configuration. This ruledef contains application filters that define the application supported by P2P protocols.

PCEF will process and install ADC rules that are received from PCRF interface, and will detect the specified applications and report detection of application traffic to the PCRF. PCRF in turn controls the reporting of application traffic.

PCEF monitors the specified applications that are enabled by PCRF and generates Start/Stop events along with the Application ID. Such application detection is performed independent of the bearer on which the ADC PCC rule is bound to. For instance, if ADC rule is installed on a dedicated bearer whereas the ADC traffic is received on default bearer, application detection unit still reports the start event to PCRF.



Important

ADC Rule support is a licensed-controlled feature. Contact your Cisco account representative for detailed information on specific licensing requirements.

In support of this feature, the following Diameter AVPs are newly added to the Charging-Rule-Definition AVP, which PCEF will receive from PCRF.

- **TDF-Application-Identifier:** It references the application detection filter which the PCC rule for application detection and control in the PCEF applies. The TDF-Application-Identifier AVP references also the application in the reporting to the PCRF.
- **Redirect-Information:** This indicates whether the detected application traffic should be redirected to another controlled address.
- **Mute-Notification:** This AVP is used to mute the notification to the PCRF of the detected application's start/stop for the specific ADC/PCC rule from the PCEF.
- **Application Detection Information:** If Mute-Notification AVP is not enclosed with charging rule report and APPLICATION_START/APPLICATION_STOP event trigger is enabled then PCEF will send Application-Detection-Information to PCRF corresponding TDF-Application-Identifier.

In addition, these two new event triggers "APPLICATION_START" and "APPLICATION_STOP" are generated for reporting purpose.

Limitations

The limitations for the ADC over Gx feature are:

- ADC does not support group of ruledefs.
- Registration of the duplicate application IDs are not supported.
- Readdress/Redirection for P2P flows will not be supported.
- Redirection happens only on transactions of GET/Response.

- Port based, IP Protocol based, and URL based applications are not supported.
- Pre-configured options (precedence, redirect-server-ip) for dynamic ADC rules are not supported.
- Simultaneous instances of an application for the same subscriber are not distinguished.
- Flow recovery is not supported for application flows.

Configuring ADC Rules over Gx

The following configuration enables ADC rules over Gx interface.

```
configure
context context_name
ims-auth-service service_name
policy-control
diameter encode-supported-features adc-rules
end
```

Notes:

- The keyword "**adc-rules**" will be available only when the feature-specific license is configured.
- For ADC 6th bit of supported feature will be set.

To disable the support for ADC Rules over Gx, use the following command:

```
[ default | no ] diameter encode-supported-features
```

GoR Name Support in TDF-Application-Identifier

ASR 5500 supports dynamic rules to be installed with GoR name as TDF-Application-Identifier. When ADC rule is installed as a dynamic rule from PCRF, the TDF-Application-Identifier can include the GoR name pre-configured in the P-GW.

If the ADC feature is enabled, PCRF can send TDF-Application-Identifier as the name of GoR predefined in the P-GW configuration.

- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated from PCRF, the PCRF can specify the GoR name configured in ECS as TDF-Application-Identifier.
- When dynamic charging-rules with the Charging-Rule-Definition AVP are activated, the PCRF can remove or modify the rule through the Charging-Rule-Definition using RAR. During rule activation or modification, the PCRF can add, modify or remove the charging-rule attributes of the rule.

The configuration changes for TDF-Application-Identifier from PCRF are listed below:

- A non-ADC dynamic rule can be changed to ADC dynamic rule by sending TDF-Application-Identifier AVP with relevant ruledef or GoR name.
ADC dynamic rule cannot be changed to non-ADC dynamic rule.
- The following AVPs will be modified and applied when received from PCRF:
 - Precedence
 - Rating-Group/Service-Identifier/Sponsor-Identity (mandatory depending on the Reporting-Level)
 - Metering-Method

- Online/Offline
 - QoS-Information
 - Monitoring-Key
 - Redirect-Information
- Dynamic route will be updated for all protocols of rules that are part of TDF-Application-Identifier GoR.
 - Any change in dynamic rule priority or TDF-Application-Identifier value will lead to sending of APP-START and APP-STOP event notifications as new rule match. If an APP-START notification was sent already before rule modification, the corresponding APP-STOP notification will not be sent.
 - Runtime deletion of associated GoR will take immediate effect and APP-STOP notification will not be sent if an APP-START was already sent. Addition of GoR at service level will need to have rules to be re-installed for the new addition to take effect for both dynamic and predefined ADC rules.

ADC Mute Customization

Earlier, 3GPP ADC over Gx did not support application MUTE status change. Once the application was muted, it was not possible to unmute it. From release 21.1, this feature introduces custom MUTE/UNMUTE functionality. ASR 5500 PCEF now supports customization to control reporting of the Application Detection Information CCRUs. For this, an AVP has been introduced with two possible values - custom MUTE and custom UNMUTE.

- A Gx message might contain both Standards based MUTE and the custom MUTE.
- Standards based MUTE is given preference over the custom MUTE/UNMUTE.
- A dynamic ADC rule can be installed and modified with a custom MUTE.
- Custom-Mute-Notification AVP can be sent by the PCRF in CCA-I and RAR.
- A dynamic ADC rule can be modified with a custom UNMUTE.
- On a custom MUTE for a given dynamic ADC rule, PCEF sends a single APPLICATION_START/ APPLICATION_STOP response for the entire application traffic rather than per flow APPLICATION_START /APPLICATION_STOP response.
- On a custom MUTE for a given dynamic ADC rule, if no APPLICATION_START has been sent prior to the custom MUTE then a single APPLICATION_START is sent on the next flow packet that hits the dynamic rule.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with the flow's 5-tuple information.
- On a custom MUTE for a given dynamic rule, the APPLICATION_START response is sent with TDF-Application-Instance-Identifier = 0.
- On a custom MUTE for a given dynamic rule, a single APPLICATION_STOP is sent when the last flow associated with the given dynamic rule is terminated. Such an APPLICATION_STOP will not contain 5-tuple information of the last flow and is sent with TDF-Application-Instance-Identifier = 0.
- On a custom UNMUTE for a given dynamic rule, APPLICATION STARTs response is matched with the given dynamic rule and then sent to all the forthcoming flows.

- There is no change in behavior for a custom UNMUTE, which has not been custom MUTED or standard MUTED before UNMUTING. APPLICATION_STARTs and APPLICATION_STOPs is continued to be sent per flow as before.
- On a custom UNMUTE, PCEF sends an APPLICATION_STOP each for all flows that terminate then onwards.
- A given dynamic rule is recovered in both SR and ICSR including the Custom MUTE/UNMUTE status. The APPLICATION_START status for a given dynamic rule is check-pointed and recovered. This ensures that an extra APPLICATION_START is not sent to the PCRF post recoveries.

Enhancement to the ADC Custom Mute/Unmute Functionality

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvd00699
Related Changes in This Release	Not Applicable
Related Documentation	Command Line Interface Reference SAEGW Administration Guide

Revision History



Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
Modified in this release.	21.2	April 27, 2017

Feature Changes

The "ADC mute customization" feature introduced custom MUTE/UNMUTE functionality to control reporting of the Application Detection Information CCRUs. With the custom MUTE PCRF AVP, the PCRF informed P-GW when to disable/enable the ADC application notifications.

This feature enhances the "ADC mute customization" feature further and report the flow activities between custom mute and unmute events. P-GW learns the flow activities between custom mute events and then reports them to PCRF after the custom unmute event has occurred on the ADC rule. It minimizes the ADC application start and stop mechanism in standard ADC mute and unmute case.

A new CLI command has been implemented at the rulebase, which when configured, reports ADC application start and stop notifications only once per rule. This helps in reducing messaging flows towards the PCRF.

Limitations

Following are the limitations of this feature:

- P-GW stores maximum of 12 learned flows per ADC rule. Once the limit 12 has been reached, P-GW forgets the oldest flow and learns about the latest flow. Once P-GW receives the custom unmute event, it notifies the PCRF about the learned notifications. P-GW sends application stop notification, if the application start notification for the flow is sent.
- Flow information stored for sending the application start notifications to the PCRF after the event of the custom unmute is not recovered.
- On LTE to WiFi handover, the values received from the PCRF for custom mute or custom unmute per ADC dynamic rule gets applied in the new RAT. If there is no value received in the handover context, the previous values before the RAT change are retained for all the ADC dynamic rules which are present.
- If the CLI command **adc notify** is enabled, then the single ADC application start and stop notification is notified to the PCRF. If there are multiple flows which match the same ADC dynamic rule, only one application start and stop notification is sent to the PCRF.
- This feature is implemented only for the dynamic rules.

How it Works

Following is the sequence of events that occur when P-GW receives packet and ADC rule event occurs from PCRF:

- 1 Packet reaches the ECS rule matching engine.
- 2 The rule matching engine checks if the ADC dynamic rule is matched. It also checks if the custom mute is applied through the PCRF or rulebase level CLI. A single application start notification is sent, if not sent earlier.
- 3 For all the subsequent flows matching the same ADC rule, application start notification is stored. These notifications are sent in the CCRU after the custom unmute event is received.

Following are some important points:

- The values received from the PCRF has the highest priority. Hence, standard mute has the highest priority than custom-mute/custom-unmute. The CLI *adc notify once* has the least priority.
- If the CLI **adc notify once** is configured at the rulebase, the converse **no adc notify** does not have any impact. To converse the CLI impact, do either of the following tasks:
 - Switch the rulebase in which the CLI **adc notify once** is not configured.

- Send the "custom unmute" for that particular dynamic rule.

Configuring the ADC Notifications

The new CLI command, **adc notify**, has been added to the active charging service mode.

When this CLI is configured, a single application start or application stop notification for the ADC flow matching per rule is sent to the PCRF. If this CLI is configured and the PCRF sends the custom mute notification, then the PCRF notification takes precedence over the standard behavior for reporting the notification.

The default value of this keyword is false. If this CLI is not configured, then no action is taken on sending the ADC notifications.

To enable or disable the feature, enter the following commands:

```
configure
  active-charging service <service_name>
    rulebase <rulebase_name>
      [no] adc notify [once]
    end
```

For configuring single notification use the following command:

adc notify once

Notes:

- **no**: Disables the ADC notifications and ADC notifications are sent as per default behavior.
- **adc**: Configures the ADC notifications.
- **notify**: Configures the application notification. If this keyword is not configured, ADC notifications are sent as per default behavior.
- **once**: Configures the application notification only once. PCRF takes the priority.

Support for TAI and ECGI Change Reporting

This section describes the overview and implementation of TAI and ECGI Change Reporting feature.

This section discusses the following topics for this feature:

- [Feature Description, on page 445](#)
- [How it Works, on page 446](#)
- [Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature, on page 447](#)

Feature Description

For activating User Location Reporting for a UE over Gx, PCRF sends RAR/CCA with the "USER_LOCATION_CHANGE (13)" event trigger. On receiving this event trigger, P-GW typically sends Change Reporting Action (CRA) Information Element (IE) with "Start Reporting" towards MME to enable the Location-Change reporting for the UE in MME.

In the current architecture, the "USER_LOCATION_CHANGE (13)" trigger is used to report the changes in User Location Information (ULI), Tracking Area Identity (TAI) and E-UTRAN Cell Global Identifier (ECGI). In release 19.4 and beyond, separate event triggers TAI_CHANGE (26) and ECGI_CHANGE (27) are supported for reporting the changes in TAI and ECGI correspondingly. CLI changes are done to display the new event triggers in show configuration commands.



Important

For TAI reporting to work, the **diameter map usage-report** CLI command must be configured in Policy Control configuration mode to use the value 33.

PCRF subscribes to the CRA event for reporting change of TAI and ECGI. P-GW sends event trigger in CCR-U only if it is subscribed by PCRF. When PCRF installs the event trigger for ECGI Change and/or TAI change, any change in ECGI and TAI (based on installed triggers) is reported.

The TAI and ECGI Change Reporting feature complies with 3GPP TS 29.212 v9.7.0. This feature is supported on Gx interface so that UE can be tracked on ECGI/TAI change and reported to PCRF. For more information on the User Location Information Reporting feature, see the administration guide for the product that you are deploying.

In releases prior to 19.3, the CRA event included in Create Session Response (CSRsp) for reporting location change was always set to START_REPORTING_ECGI (4).

In release 19.4 and beyond, the CRA value varies based on the event triggers received from PCRF.

Change Reporting Support Indication (CRSI) and ULI are also supported in Bearer Resource Command.

P-GW sends the ULI received in Delete Bearer Command from MME to PCRF when the corresponding Delete Bearer Response is received. When the ULI is included in both Delete Bearer Command and Delete Bearer Response, the ULI in Delete Bearer Response is sent to the PCRF. In the absence of ULI in Delete Bearer Response, then the ULI received in Delete Bearer Command is sent to PCRF.

Relationships to Other Features

This feature has a dependency on USAGE_REPORT value of Event-Trigger AVP. This feature works only when the value of USAGE_REPORT is set to 33. This can be achieved using the **diameter map usage-report** CLI command in Policy Control configuration mode.

How it Works

P-GW sends Event Trigger value based on the event trigger detected by P-GW in CCR-U. P-GW sends Event Trigger and ULI Type in CCR-U to PCRF as per the following table.

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ULI_CHANGE	6	TAI_CHANGE or ECGI_CHANGE	Event Trigger: ULI_CHANGE ULI Type: TAI + ECGI
TAI_CHANGE	3	TAI_CHANGE	Event Trigger: TAI_CHANGE ULI Type: TAI

Event Trigger from PCRF	CRA Value	Event Detected at P-GW	What to Inform PCRF
ECGI_CHANGE	4	ECGI_CHANGE	Event Trigger: ECGI_CHANGE ULI Type: ECGI
ULI_CHANGE + TAI_CHANGE	6	TAI_CHANGE	Event Trigger: ULI_CHANGE+ TAI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + ECGI_CHANGE	6	ECGI_CHANGE	Event Trigger: ULI_CHANGE + ECGI_CHANGE ULI Type: TAI+ECGI
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: ULI_CHANGE + TAI/ECGI CHANGE ULI_Type: TAI+ECGI
TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI has changed	Event Trigger: TAI_CHANGE/ECGI_CHANGE ULI_Type: TAI+ECGI
For combinations not specifically mentioned above	6		Event Trigger: ULI_CHANGE ULI_Type: TAI+ECGI

Limitations

TAI and ECGI Change Reporting feature is supported only when *diameter map usage-report* CLI command is configured as 33.

Monitoring and Troubleshooting the TAI and ECGI Change Reporting Feature

This section provides information regarding show commands and/or their outputs in support of the TAI and ECGI Change Reporting feature.

show ims-authorization sessions full all

The following fields are added to the output of this show command in support of this feature:

- TAI-Change - Displays this event trigger when TAI has changed for a subscriber session.
- ECGI-Change - Displays this event trigger when ECGI has changed for a subscriber session.

show ims-authorization service statistics all

The following statistics are added to the output of this show command in support of this feature:

- TAI Change - Displays the total number of times P-GW has reported TAI_CHANGE (26) event trigger to PCRF.
- ECGI Change - Displays the total number of times P-GW has reported ECGI_CHANGE (27) event trigger to PCRF.

Location Based Local-Policy Rule Enforcement

This section describes the overview and implementation of Location-based Local-Policy (LP) Rule Enforcement feature.

This section discusses the following topics for this feature:

- [Feature Description, on page 448](#)
- [How it Works, on page 449](#)
- [Configuring Location Based Local Policy Rule Enforcement Feature, on page 450](#)
- [Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature, on page 452](#)

Feature Description

This feature is introduced to activate different predefined rules for different E-UTRAN Cell Global Identifiers (ECGIs) when the subscriber is connected to a corporate APN. The subscriber has to explicitly bring down the connection with the corporate APN and re-establish session with Internet APN when out of the company area. It is assumed that corporate APN does not use PCRF and use only Local-Policy. In this case, all calls matching the APN is directed to the Local-Policy.



Important

For this feature to work, the license to activate Local-Policy must be configured. For more information on the licensing requirements, contact your local Cisco account representative.

To activate different predefined rules for ECGI, Local-Policy configurations are enhanced to support:

- Configuration and validation of a set of ECGIs
- Installation of ECGI_CHANGE event trigger through Change Reporting Action (CRA) event
- Detection of ECGI_CHANGE event

This feature supports the following actions to be applied based on the ECGI match with Local-Policy ruledef condition:

- Enable a redirect rule on ECGI_CHANGE event notification when the ECGI belongs to a certain group
- Enable a wild card rule for any other ECGIs

Relationships to Other Features

This feature has a dependency on TAI and ECGI Change Reporting feature, which provides a framework to report ECGI-Change from session manager module to IMSA/Local-Policy module.

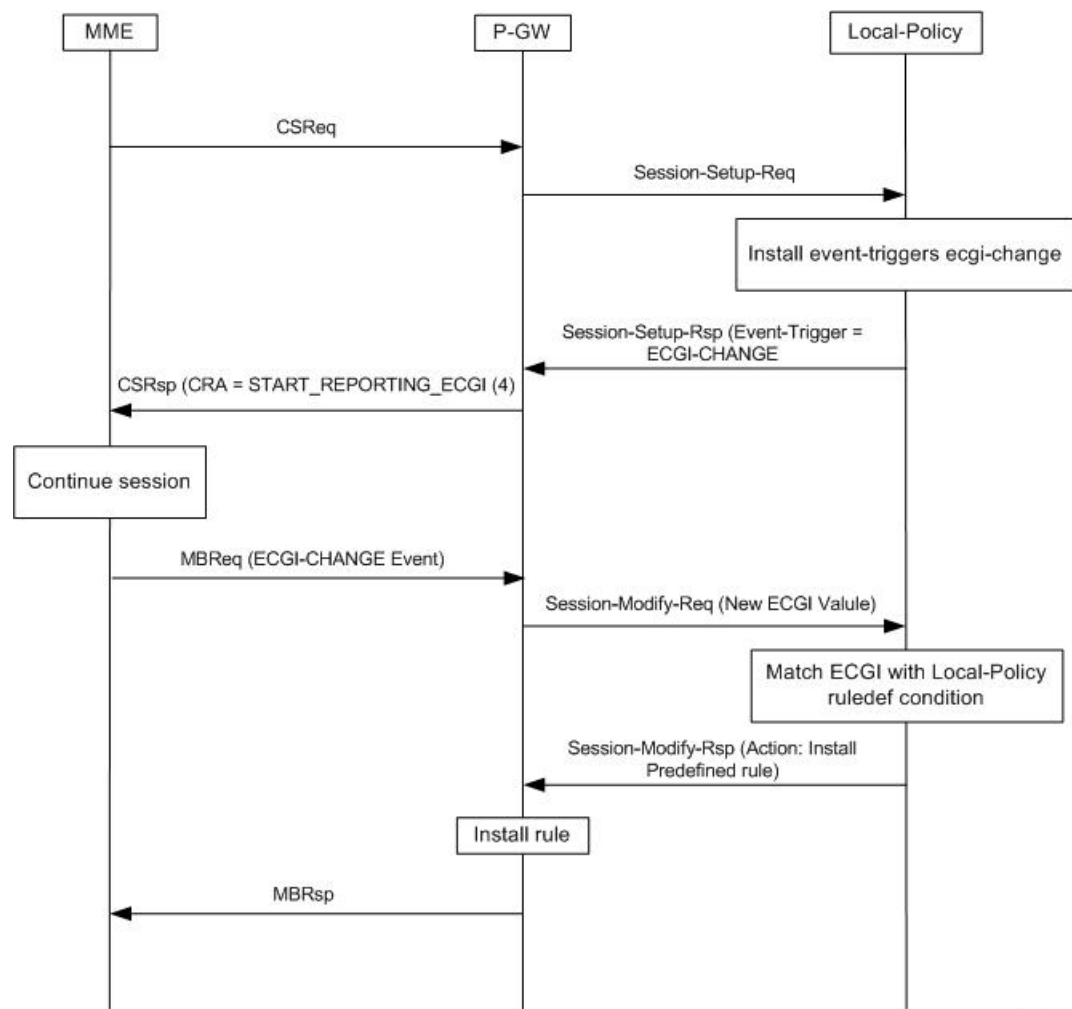
How it Works

This section describes how the Local Policy Rule selection and enforcement happens based on ECGI-CHANGE event trigger.

Flows

The following figure describes how the ECGI-CHANGE event is being handled in Local-Policy, MME and P-GW.

Figure 64: ECGI-CHANGE Event Handling



412887

When a new call is established the ECGI-CHANGE event trigger is sent from Local-Policy. P-GW requests the MME for ECGI reporting by sending CRA of 4 in Create Session Response (CSRsp). MME informs the P-GW of ECGI Change through Change Notification request/Modify Bearer Request (MBReq). Local-Policy configuration at P-GW will handle the ECGI-CHANGE event and take appropriate action based on the ECGI group to which the new ECGI belongs. One action could be to activate a certain redirect rule when ECGI belongs to a certain group, and other action could be to enable a wildcard rule for any other ECGI.

Limitations

This section identifies the known limitations of this feature.

- ECGI Change detection and triggering is a pre-requisite for this feature.
- This feature is supported for Local-Policy-only (lp-only) mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF. That is, this feature does not work in Local-Policy fallback mode and dual mode wherein both PCRF and Local-Policy co-exist.

Configuring Location Based Local Policy Rule Enforcement Feature

This section provides the configuration of parameters within Local-Policy to enable rule enforcement based on ECGI-Change event notification.

Configuring ECGI Change Trigger

Use the following configuration to install ECGI-Change trigger from local-policy.

configure

local-policy-service *service_name*

actiondef *actiondef_name*

action *priority* **event-triggers** **ecgi-change**

exit

eventbase *default*

rule *priority* **event** **new-call** **ruledef** *ruledef_name* **actiondef** *actiondef_name* [**continue**]

end

Notes:

- **priority** *priority*: Specifies a priority for the specified action. *priority* must be unique and an integer from 1 to 2048.
- **ecgi-change**: This keyword specifies to install ECGI-CHANGE event trigger. If enabled, ECGI-CHANGE event trigger is sent from local-policy.
- This CLI command is configured in local-policy if operator wants to enable ECGI-Change notification in MME by sending a CRA value.

Applying Rules for ECGI-Change Event

Use the following configuration to enable ECGI Change detection and take specific action for ECGI-CHANGE event reported by MME.

configure

local-policy-service *service_name*

eventbase *eventbase_name*

rule *priority* **event** **ecgi-change** **ruledef** *ruledef_name* **actiondef** *actiondef_name* [**continue**]

```
|
  end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified rule. *priority* must be unique and an integer from 1 to 2048.
- **ruledef** *ruledef_name*: Associates the rule with a specific ruledef. *ruledef_name* must be an existing ruledef within this local QoS policy service.
- **actiondef** *actiondef_name*: Associates the rule with a specific actiondef. *actiondef_name* must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.
- **ecgi-change**: Enables a new event to detect ECGI-CHANGE and applies specific action for the ECGI-CHANGE event as defined in actiondef configuration.
- **continue**: Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Enforcing Local Policy Rule based on ECGI Value

Use the following configuration to apply rules based on the ECGI value received in ECGI-Change event notification by MME.

configure

```
  local-policy-service service_name
```

```
    ruledef ruledef_name
```

```
      condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq | ge | gt | le | lt | match | ne |
nomatch } regex | string_value | int_value | set }
    end
```

Notes:

- **priority** *priority*: Specifies a priority for the specified condition. *priority* must be unique and an integer from 1 to 2048.
- **ecgi mcc mcc_num mnc mnc_num eci**: Configures ECGI with values for MCC, MNC and ECI.
 - **mcc** *mcc_num* : MCC is a three digit number between 001 to 999. It is a string of size 3 to 3.
 - **mnc** *mnc_num* : MNC is a two/three digit number between 01 to 999. It is a string of size 2 to 3.
 - **eci**: ECI is a hexadecimal number between 0x1 to 0xffffffff. It is a string of size 1 to 7.
- This CLI command is configured in local-policy if operator wants to take specific action based on certain ECGI value received in ECGI-Change event notification by MME.

Verifying the Location Based LP Rule Enforcement Configuration

Use the following command to verify the configuration of this feature.

show configuration context



Important

This feature is supported for Local-Policy-only mode wherein, all requests and responses within a particular APN directly go to Local-Policy without contacting PCRF.

Here is an example configuration for this feature.

```

configure
  context source
    apn corporate-apn
    ims-auth-service LocalPolicy_1
  exit
exit
end
configure
  local-policy-service LocalPolicy_1
    ruledef any-imsi
      condition priority 1 imsi match *
    exit
    ruledef ecgi-group
      condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
    exit
    actiondef ecgi-trigger
      action priority 1 event-triggers ecgi-change
    exit
    actiondef ecgi-redirect-rule
      action priority 1 activate-rule namerule-1
    exit
    eventbase default
      rule priority 1 event new-call ruledef any-imsi actiondef ecgi-trigger
      rule priority 2 event ecgi-change ruledef ecgi-group actiondef ecgi-redirect-rule
      rule priority 3 event location-change ruledef ecgi-group actiondef ecgi-redirect-rule
    exit
  exit
end

```

Monitoring and Troubleshooting the Location Based LP Rule Enforcement Feature

This section provides information regarding show commands and/or their outputs in support of the Location Based Local Policy Rule Enforcement feature.

Use the following CLI commands to troubleshoot if any issue is encountered with this feature.

```

show configuration context
logging filter active facility local-policy level debug
show local-policy statistics
show active-charging sessions full

```

show local-policy statistics summary

The following statistics are added to the output of this show command to support the ECGI-CHANGE event trigger installation:

- Event Statistics:
 - ECGI Change - Displays the number of ECGI-CHANGE event triggers that has been received by Local-Policy.
- Variable Matching Statistics

- ECGI - Displays the number of times the ECGI is matched and the specific action is applied based on the event.

Gx Support for GTP based S2a/S2b

In releases prior to 18, for WiFi integration in P-GW, Gx support was already available for GTP based S2a/S2, but the implementation was specific to a particular customer.

In 18 and later releases, the Gx support for GTP based S2a/S2 interface is extended to all customers. This implementation is in compliance with standard Rel.8 Non-3GPP specification part of 29.212, along with C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CRs from Rel.10/Rel.11.

As part of this enhancement, the following changes are introduced:

- AVP support for TWAN ID is provided
- TWAN-ID is added to r8-gx-standard dictionary

Gx-based Virtual APN Selection

This section describes the overview and implementation of Gx based Virtual APN Selection feature.

This section discusses the following topics for this feature:

- [Feature Description, on page 453](#)
- [Configuring Gx based Virtual APN Selection Feature, on page 454](#)
- [Monitoring and Troubleshooting the Gx based Virtual APN Selection, on page 455](#)

Feature Description

Overview

The current implementation supports Virtual APN (VAPN) Selection through RADIUS or local configuration. In Release 19, ASR 5500 uses PCRF and Gx interface for Virtual APN selection to achieve signaling reduction.

A new supported feature "**virtual-apn**" with feature bit set to 4 is added to the IMSA configuration. This configuration enables Gx based Virtual APN Selection feature for a given IMS authorization service. When this configuration is enabled at P-GW/GGSN, then P-GW/GGSN advertises this feature to PCRF through the Supported-Features AVP in CCR-I. When the VAPN is selected, then the PCRF rejects the CCR-I message with the Experimental-Result-Code AVP set to 5999 (DIAMETER_GX_APN_CHANGE), and sends a new APN through the Called-Station-Id AVP in CCA-I message. The existing call is then disconnected and reestablished with the new virtual APN. Note that the Experimental Result Code 5999 will have the Cisco Vendor ID.



Important

Enabling this feature might have CPU impact (depending on the number of calls using this feature).

License Requirements

This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Limitations

The following are the limitations of this feature:

- Virtual APN supported feature negotiation, Experimental Result Code (5999), Called-Station-Id AVP should be received to establish the call with new virtual APN. When any one of conditions is not met then the call will be terminated.
- Failure-handling will not be taken into account for 5999 result-code when received in the CCA-I message.
- When the Experimental Result Code 5999 is received in the CCA-U then failure-handling action will be taken.
- If the Called-Station-Id AVP is received in CCA-U or CCA-T, then the AVP will be ignored.
- If virtual-apn is received in local-policy initiated initial message then the call will be terminated.
- When PCRF repeatedly sends the same virtual-apn, then the call will be terminated.

Configuring Gx based Virtual APN Selection Feature

The following section provides the configuration commands to enable the Gx based Virtual APN Selection.

```
configure
context context_name
    ims-auth-service service_name
        policy-control
            diameter encode-supported-features virtual-apn
        end
end
```

Notes:

- **virtual-apn**: This keyword enables configuration of Gx-based Virtual APN Selection feature. By default, this feature is disabled.
- This keyword is license dependent. For more information, contact your Cisco account representative.

Verifying the Gx based Virtual APN Configuration

Use the following command in Exec mode to display whether the Gx based Virtual APN Selection feature is configured as part of the Supported-Features AVP.

```
show ims-authorization sessions full all
```

The "Negotiated Supported Features" field in this show command output displays the configuration status. This supported feature is displayed only when the feature license is configured.

Monitoring and Troubleshooting the Gx based Virtual APN Selection

This section provides information regarding show commands and/or their outputs in support of this feature.

show ims-authorization policy-control statistics

The following field has been added to the output of this show command to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- **Gx APN Change**

For descriptions of this statistics, see the *Statistics and Counters Reference* guide.

Debugging Statistics

Use the following command to debug the Gx based Virtual APN calls.

show session subsystem facility sessmgr debug-info

This command displays the detailed statistics associated with the Gx-based VAPN feature. For example, number of Gx VAPN received, number of AAAMGR/SGX/DHCP messages after enabling Gx VAPN, and Gx VAPN calls setup time.

Bulk Statistics for Gx based Virtual APN Selection Feature

IMSA Schema

The following new bulk statistic variable is added to the IMSA schema to track the number of times the PCRF sends the Diameter Experimental Result Code (5999) when a new virtual APN is selected.

- dpca-expres-gx-apn-change

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

System Schema

The following new disconnect reason is added to the System schema to track the number of times a P-GW/GGSN/SAEGW session was disconnected due to validation failure of virtual APN received from PCRF.

- gx-vapn-selection-failed (618)

For descriptions of this variable, see the *Statistics and Counters Reference* guide.

Graceful Handling of RAR from Different Peers

In StarOS Gx architecture, every Diameter session is associated with a Primary and a Secondary peer when host select is configured at the IMSA service. The behavior for processing RAR prior to release 20 is as follows:

- If the RAR is received from the Primary peer for the session, the RAR is responded using the Primary peer connection.

- If the RAR is received from a Secondary peer for the session, host-switch takes effect. This results in the RAA (and any further session signaling) happening via the Secondary peer.
- If the RAR is received via a third peer which is neither the Primary nor the Secondary peer for the session, the RAR is dropped.

In certain networks where PCRF and PCEF are connected through multiple DRAs the PCRF may select the DRA in a round-robin fashion and the RAR for a session may come from a peer which is neither Primary nor Secondary. In order to handle such a scenario, the ability to respond to the RAR received from a non-primary and non-secondary peer was added. In this case, the RAR is answered via the peer from which RAR was received. However any future signaling for the session will still occur via the previously communicating peer. If the RAR is received via the secondary peer, the host-switch occurs and the behavior remains unchanged. In order to be able to process the RAR from a third peer, that peer must be configured in the Diameter endpoint configuration. Further, this issue is seen only when host select is configured at IMSA service. When the host selection happens at endpoint level, this issue is not seen.

Assume there are three DRAs and they are configured as shown in the sample configuration below:

```
configure
context test
  diameter endpoint Gx
    ...
    peer DRA1 realm realmName address 192.168.23.3
    peer DRA2 realm realmName address 192.168.23.3 port 3869
    peer DRA3 realm realmName address 192.168.23.3 port 3870
  exit
  ims-auth-service imsa-Gx
    policy-control
      diameter host-select row-precedence 1 table 1 host DRA1 secondary host DRA2
    end
```

Without the feature, when RAR is received from DRA3, it is rejected. With the feature enabled, RAR from DRA3 is responded via DRA3 only and Peer switch will not occur in this case and subsequent messaging will be sent through DRA1 or DRA2 if any prior peer switch had happened.

Limitations

This section identifies the limitations for this feature.

- RAR will be rejected when received from different origin host.
- RAR will be rejected when received from a DRA not configured in Diameter endpoint.

NetLoc Feature Enhancement

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality.

Feature Description



Important

This is a license controlled feature. Netloc feature license key is required to be enabled. Contact your Cisco account representative for information on how to obtain a license.

This feature adds compliance with 3GPP standard R13 version to the existing NetLoc feature functionality. Using this NetLoc feature, the IMS network can retrieve location information of the UE from the access or LTE network. This enhances the location related functionality and charging based on the location information.

This feature introduces the following behavior changes:

- Assuming that NetLoc feature is enabled on chassis and Access Network Information (ANI-45) Event trigger is installed, following behavior changes have been introduced:

Table 30: Gx Interface Behavior Change Towards PCRF

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15 (AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15 (AT&T))
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with only New ULI parameter.	Create Bearer Response is received with only New ULI parameter.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule install request.	Create Bearer Response is received with No ULI parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Update Bearer Response is received with only New ULI parameter.	New ULI parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Update Bearer Response is received with No ULI parameter.	Old ULI parameter is sent towards the PCRF in the CCR-U message.	PLMN-id in 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '0 - ULI' is received in the charging rule modify request.	Delete Bearer Response is received with only New ULI parameter and No MS TZ parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New ULI is sent towards the PCRF in the CCR-U message.
RAI AVP with '0 - ULI' is received in the charging rule Modify request.	Delete Bearer Response is received with No ULI parameter and No MS TZ parameter.	Old ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	PLMN-id in the 3GPP-SGSN-MCC-MNC AVP is sent towards the PCRF.
RAI AVP with '1 -MSTZ' is received in the charging rule install request.	Create Bearer Response is received with only new MS TZ parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.

PCRF Gx Interface Interaction	Access Side Interaction	ULI & MS TZ Behavior Before 21.1 Release(Standard Gx-R8/Custom15(AT&T))	ULI & MS TZ Behavior Change(Standard Gx-R8/Custom15(AT&T))
RAI AVP with '1 - MSTZ' is received in the charging rule install request.	Create Bearer Response is received with No MS TZ parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Update Bearer Response is received with only New MS TZ parameter.	New MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Update Bearer Response is received with No MS TZ parameter.	Old MS TZ parameter is sent towards the PCRF in the CCR-U message.	No change in the behavior.
RAI AVP with '1 -MSTZ' is received in the charging rule modify request.	Delete Bearer Response is received with only New MS TZ parameter.	Old ULI and New MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only New MS TZ is sent towards the PCRF in the CCR-U message.
RAI AVP with '1 -MSTZ' is received in the charging rule Modify request.	Delete Bearer Response is received with No MS TZ parameter.	New ULI and old MS TZ parameters are sent towards the PCRF in the CCR-U message.	Only old MS TZ is sent towards the PCRF.
Nothing is received.	Delete Session Request is received with New ULI and New MS TZ parameters.	New ULI and New MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with New ULI and No MS TZ parameter.	New ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.
Nothing is received.	Delete Session Request is received with No ULI and No MS TZ parameter.	Old ULI and Old MS TZ parameters are sent towards the PCRF in the CCR-T message.	No change in the behavior.

**Important**

ULI and ULI timestamp is considered as paired. If the ULI timestamp is forwarded, it is forwarded and received with the ULI. If the ULI is received and the ULI timestamp is not received, then that P-GW does not forward the old timestamp.

- Inclusion of AVP support of NETLOC-ACCESS-NOT-SUPPORTED on Gx interface. This inclusion of AVP is based on the below conditions:
 - RAT type is other than E-UTRAN, UTRAN, WCDMA, GPRS, GERAN, and W-LAN
 - IP CAN type is other than 3GPP EPS, GPRS, and non 3GPP EPS
 - Re-Auth-Request is received with Required-Access-Info AVP.
 - NetLoc feature is enabled on the chassis.
 - Event-Trigger ACCESS_NETWORK_INFO_REPORT (45) is installed.

Before Release 21.1 Behavior (Standard Gx-R8/Custom15(AT&T))	New Behavior(Standard Gx-R8/Custom15(AT&T))
Earlier, if IP-CAN type or RAT type was not support NETLOC, P-GW(PCEF) ignored RAI received from the PCRF.	New AVP NetLoc-Access-Support has been added in the Re-Auth-Answer message in the R8-Gx-standard and the Custom15 Gx Dictionary.

• **Table 31: Behavior Change Regarding LastUserLocationInformation AVP and LastMSTimeZone AVP**

P-GW CDR Behavior	Post 21.1 Release, Behavior in Custom 35/Custom 24/Custom 48 Dictionaries	Custom52 Dictionary (standard compliance new dictionary)/ Custom 35 Dictionary (Customer Specific)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of P-GW CDR generation.	ULI is recorded as LastUserLocationInformation AVP in the P-GW CDR generation. (AVP is not controlled using the CLI command.)
MS TZ is received in the Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of P-GW CDR generation.	MS TZ is recorded as LastMSTimeZone AVP in the P-GW CDR generation. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause. AVP is not controlled using the CLI command.

S-GW CDR behavior	Post 21.1 Release behavior in Custom 35/Custom 24 Dictionary	Custom24 Dictionary (standard dictionary)/ Custom 35 Dictionary (AT&T)
ULI is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	ULI was not part of CDR generation.	ULI is Recorded as LastUserLocationInformation AVP in the S-GW CDR generation. The attribute is controlled using a CLI command.
MS TZ is received in Delete Bearer Command/Delete Bearer Request /Delete Session Request.	MS TZ was not part of CDR generation.	MS TZ is Recorded as LastMSTimeZone AVP in S-GW CDR generation. The attribute is controlled using a CLI command. CDR is released as Normal Release. MS TZ is not detected in this case as full trigger and does not release extra CDR with MS TZ changes cause.

Limitations

- 1 This feature enhancement is applicable only for S-GW, P-GW, and SAEGW. For GGSN and SGSN, there is no change in the behavior of the NetLoc feature.
- 2 The attributes **Last-MS-Timezone** and **Last ULI attributes** have been added in the dictionaries custom24 and custom35 for S-GW CDR generation only.
- 3 The keywords **last-ms-timezone** and **last-uli** added to the CLI command **gtp attribute** are applicable and limited to only S-GW CDR generation.
- 4 **Last-MS-Timezone** and **Last ULI attributes** added in dictionary custom35 (customer specific dictionary) and custom52 (3GPP R13 standard compliance) are applicable and limited to P-GW CDR generation only. These attributes are not CLI controlled.

Command Changes

gtp-attribute

This CLI command allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values. The keywords **last-ms-timezone** and **last-uli** have been added to this CLI command to control attribute while CDR generation.

**Important**

The keywords added are applicable only for S-GW CDR. They are not applicable for P-GW CDR.

```
configure
  context <context_name>
    gtpv group group_name
      gtpv attribute { last-ms-timezone | last-uli | .. }
      [no | default ] gtpv attribute { last-ms-timezone | last-uli | .. }
    end
```

Notes:

- **no:** Removes the configured GTPV attributes from the CDRs.
- **default:** Sets the default GTPV attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.
- **last-ms-timezone:** Sets the "Last MS-Timezone" in the CDR field. This option would be disabled when the default option is used.
- **last-uli:** Sets the "Last ULI" in the CDR field. This option would be disabled when the default option is used.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

- Last-MS-Timezone present
- Last-User Location Information present

show gtpv group name *group_name*

This command has been modified to display the following output:

```
Last-MS-Timezone present: yes
Last-User Location Information present:
yes
```

RAN-NAS Cause Code Feature Enhancement

This chapter describes the RAN-NAS Cause Code Feature Enhancement.

Feature Description



Important

This is a license controlled feature. You must enable the existing license of NPLI. Contact your Cisco account representative for information on how to obtain a license.

This feature introduces support for 3GPP RAN/NAS cause code IE for "Failed Create Bearer Response", "Failed Updated Bearer Response", and "Delete Bearer Response" at the Gx interface, the P-GW, and S-GW CDRs. This will enable the operator to get detailed RAN/NAS release cause code information from the access network. RAN/NAS cause can be received from the access side in either of the following messages:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

This support of 3GPP Release 12 RAN/NAS cause IE on the S4, S11, S5, and S8 interfaces exists for "Delete Session Request" and "Delete Bearer" command through private extension as well as Standard IE for customer specific dictionaries Gx- dpca-custom15 and Gz-Custom35.

However, RAN/NAS cause received in the "ERAB creation Failure", "ERAB modification Failure", and "ERAB release indication" messages were not processed at the S-GW and P-GW. Hence, it was also not forwarded to the PCRF by P-GW neither populated in the P-GW and S-GW CDRs. With this feature enhancement, support has been added to process the RAN/NAS cause codes at the S-GW (S4,S11 interface) and P-GW (S5,S8 interface) for the "Create bearer response", "Update bearer response", and "Delete bearer response". Also, RAN/NAS cause codes will be forwarded to the PCRF by the P-GW and will be populated in the P-GW and S-GW CDRs.

There is no requirement to add the support for the 3GPP Release 12 RAN/NAS cause IE received in the private extension for "Create Bearer Response", "Update Bearer Response", and "Delete Bearer Response". Private extension support for 3GPP Release 12 cause code IE in "Delete Session Request" and "Delete Bearer Command" will continue to be supported.

This feature enhancement introduces the following RAN/NAS cause IE behavior changes at the Gx interface for dpca-custom15 dictionary and at Gz interface for custom35 dictionary.

Table 32: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if received it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. So if it is received, it is ignored and is not forwarded to the PCRF.
	No Resources	CCR-U
	Available	Important If the UE-initiated (MBC) bearer modification fails with the GTP cause "NO RESOURCES AVAILABLE", then P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of the CCR-T message.
	Context Not Found	If the update bearer response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF.
	Other GTP Causes	CCR-U
Delete Bearer Response	Temporarily rejected due to HO in progress	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. So if this cause is received, it is ignored and is not forwarded to the PCRF. Important As per existing design of S-GW, if "Delete Bearer Response" is received with GTP cause "Temporarily rejected due to handover/ TAU/ RAU procedure in progress" it changes GTP cause to "Request Accepted" and forwards it to the P-GW. In this case, if RAN/NAS cause is received in the "Delete Bearer Response", S-GW will forward it to the P-GW. And at the P-GW since "Delete Bearer Response" is received with the GTP cause "Request Accepted" hence RAN/NAS cause is forwarded to the PCRF and populated in the P-GW CDR. This behavior will be seen for SAEGW and S-GW + P-GW combination call.
	Accepted / Other GTP CCR-U Causes	Important If RAN/NAS cause is received in the delete bearer response that is initiated by the network through RAR/CCA-U, then P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".

Table 33: Gz Interface Requirements for RAN/NAS Cause

Message	S-GW CDR	P-GW CDR
Delete Session Request	Yes	Yes
Delete Bearer Command	Yes	Yes NOTE: RAN/NAS cause if received in delete bearer response will overwrite the RAN/NAS cause received in delete bearer command
Failed Create Bearer Response	No	No
Failed Update Bearer Response	No	No
Delete Bearer Response	No	Yes

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause over S2a and S2b interfaces is not supported.
- Support of RAN/NAS cause information has not been added for standard Gx and Gz dictionaries.
- P-GW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, these are two NAS causes, only first NAS cause will be populated at the Gx interface and in the CDRs as only one NAS is allowed.
- As per spec 32.251 Table 5.2.3.4.1.1 and Table 5.2.3.4.2.1, there is no trigger to generate the S-GW CDRs and P-GW CDRs for failed create bearer response and failed update bearer response. Hence, RAN/NAS cause received in "Failed Create Bearer" response and "Failed Update Bearer" response will not be sent to the Gz interface.
- In "Delete Bearer" scenario, S-GW CDRs are generated immediately after receiving "Delete Bearer" request. Hence, RAN/NAS cause received in the "Delete Bearer" response is not populated in the S-GW CDRs.
- If RAN/NAS cause is received in the "Delete Bearer" response that is initiated by the network through RAR/CCA-U, P-GW will not send CCR-U to the PCRF to report the RAN/NAS cause. This support is introduced in spec 29.212 release 13.5 with "Enhance RAN/NAS" feature".
- If the RAN-NAS-Cause feature is supported, only RAN/NAS cause is forwarded to PCRF . ANI information will be forwarded only when NetLoc feature is enabled. Below table describes various scenarios,

Scenario	RAN/NAS Cause Behavior	ANI Behavior
IP-CAN Bearer Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to bearer termination, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received during bearer termination is populated in the CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in Gx CCR-I/CCA-I).
IP-CAN Session Termination	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in the Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to session termination, in the RAN-NAS-Release-Cause AVP at the command level.	ANI information received during session termination is populated in CCR-T, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in the CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).
PCC Rule Error Handling	If the RAN-NAS-Cause feature is supported (If Netloc-ran-nas-cause CLI is configured and Supported-Features = RAN-NAS-CAUSE was asserted in Gx CCR-I/CCA-I), PCEF will include the received RAN cause and/or the NAS cause due to rule installation/ activation/ modification failure, in the RAN-NAS-Release-Cause AVP included in the Charging-Rule-Report AVP.	ANI information received due to rule installation/activation/modification failure is populated in CCR-U, if Required-Access-Info was asserted when one or more of the failed charging rules installation request was received in CCA-U/RAR (If Netloc CLI is configured and Supported-Features = Netloc was asserted in the Gx CCR-I/CCA-I).

Command Changes

diameter encode-supported-features netloc netloc-ran-nas-cause

The behavior of this CLI command has been modified in this feature enhancement.

Previous Behavior: To enable the RAN/NAS Cause feature, it was mandatory to enable the NetLoc feature. For this, it was mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause**.

New Behavior: Now, you can enable the RAN/NAS feature without configuring the NetLoc feature. This implied that it is not mandatory to configure the **netloc** keyword in the CLI command **diameter encode-supported-features netloc netloc-ran-nas-cause**.

```
configure > context context_name > ims-auth-service service_name > policy-control
diameter encode-supported-features netloc netloc-ran-nas-cause
```

Session Disconnect During Diamproxy-Session ID Mismatch

This section describes how to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

This section discusses the following topics for this feature:

- [Feature Description, on page 466](#)
- [Configuring System to Delete Diamproxy-Session ID Mismatched Sessions, on page 466](#)
- [Monitoring and Troubleshooting the Mismatched Session Deletion Feature, on page 467](#)

Feature Description

During rapid back-to-back ICSR switchovers or extensive multiple process failures, the Diameter proxy-Session manager mapping information is not preserved across ICSR pairs. This mismatch in the Diameter proxy-Session ID results in rejection of RAR with 5002 - DIAMETER_UNKNOWN_SESSION_ID cause code. This behavior impacts the VoLTE call setup procedure. Hence, this feature is introduced to clear the subscriber sessions that are impacted due to the mismatch in the Diameter proxy-session manager mapping. New CLI configuration is provided to control the behavior and new bulk statistic counter is supported to report the Diamproxy-Session ID mismatch.

The bulk statistic counter will be incremented only when session is cleared upon receiving RAR message with 5002 result code and detecting session-ID Diamproxy mapping mismatch. A Delete Bearer Request is sent to S-GW with a Reactivation Requested as the cause code while suppressing the CCR-T from being sent to PCRF. So, the subscriber reattaches immediately without impacting the subsequent VoLTE calls, encountering only one failure instead of manual intervention.



Important

This enhancement is applicable only to IMS PDN so that there is a limit of one failure when encountering this situation instead of manual intervention. This is applicable to only the Gx RARs.

Configuring System to Delete Diamproxy-Session ID Mismatched Sessions

The following section provides the configuration commands to enable the system to clear the subscriber sessions that are impacted due to the mismatch in Diamproxy grouping information and Session ID.

Clearing Mismatched Subscriber Sessions

Use the following configuration commands to configure the system to disconnect the subscriber sessions based on signaling trigger when session ID and Diamproxy mismatch is identified.

```
configure
context context_name
ims-auth-service service_name
policy-control
diameter clear-session sessid-mismatch
end
```

- **sessid-mismatch**: Clears the session with mismatched session ID. This CLI configuration is optional.
- The default configuration is **no diameter clear-session**. By default, the sessions will not be cleared.

Verifying the Configuration to Delete Mismatched Sessions

Use the following command to verify the configuration status of this feature.

show ims-authorization service name service_name
service_name must be the name of the IMS Authorization service configured for IMS authentication.

This command displays all the configurations that are enabled within the specified IMS authorization service. The "Session-Id Mismatch Clear Session" field can be used to determine whether this feature is enabled or disabled.

```
[local]st40# show ims-authorization service name servicel
Context: test
IMS Authorization Service name: servicel
Service State: Enabled
Service Mode: Single Interface Policy and Charging
...
Diameter Policy Control:
Endpoint: gx
Origin-Realm: xyz.com
Dictionary: standard
Supported Features:
    3gpp-r9
...
Host Selection: Table: 1 Algorithm: Round-Robin
Host Reselection Subscriber Limit: Not Enabled
Host Reselection Interval: Not Enabled
Sgsn Change Reporting: Not Enabled
Session-Id Mismatch Clear Session: Enabled
3GPP R9 Flow Direction Compliance: Not Enabled
Host Selection Table[1]: 1 Row(s)
Precedence: 1
...
```

Monitoring and Troubleshooting the Mismatched Session Deletion Feature

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed for any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization service name <service_name>** CLI command. If not enabled, configure the **diameter clear-session sessid-mismatch** CLI command and check if it works.
- Collect the output of **show ims-authorization policy-control statistics debug-info** and **show diameter statistics proxy debug-info** commands and analyze the debug statistics.

- Check the system logs that are reported while deleting the affected sessions. For further analysis, contact Cisco account representative.

show ims-authorization service name

A new field "Session-Id Mismatch Clear Session" is added to the output of this show command to indicate whether this feature is enabled or disabled within the specified IMS authorization service.

IMS Schema

The following bulk statistic variable is added to this schema to report the Diamproxy-Session ID mismatch.

- **dpca-rar-dp-mismatch** - This counter displays the total number of sessions cleared while receiving RAR because of session-ID Diamproxy mapping mismatch.

Support for Negotiating Mission Critical QCIs

This section describes the overview and implementation of the Mission Critical QCIs Negotiation feature.

This section includes the following topics:

- [Feature Description, on page 468](#)
- [Configuring DPCA for Negotiating Mission Critical QCIs, on page 469](#)
- [Monitoring and Troubleshooting the Mission Critical QCI, on page 469](#)

Feature Description

To support Mission Critical (MC) Push to Talk (PTT) services, a new set of standardized QoS Class Identifiers (QCIs) (65, 66, 69, 70) have been introduced. These are 65-66 (GBR) and 69-70 (non-GBR) network-initiated QCIs defined in 3GPP TS 23.203 v13.6.0 and 3GPP TS 23.401 v13.5.0 specifications. These QCIs are used for Premium Mobile Broadband (PMB)/Public Safety solutions.



Important

The MC-PTT QCI feature requires Wireless Priority Service (WPS) license to be configured. For more information, contact Cisco account representative.

Previous Behavior: The gateway accepted only standard QCIs (1-9) and operator defined QCIs (128-254). If the PCRF sends QCIs with values between 10 and 127, then the gateway rejects the request. MC QCI support was not negotiated with PCRF.

New Behavior: PCRF accepts the new standardized QCI values 69 and 70 for default bearer creation and 65, 66, 69 and 70 for dedicated bearer creation.

For this functionality to work, a new configurable attribute, **mission-critical-qcis**, is introduced under the **diameter encode-supported-features** CLI command. When this CLI option is enabled, the gateway allows configuring MC QCIs as a supported feature and then negotiates the MC-PTT QCI feature with PCRF through Supported-Features AVP.

The gateway rejects the session create request with MC-PTT QCIs when the WPS license is not enabled and Diameter is not configured to negotiate MC-PTT QCI feature, which is part of Supported Feature bit.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring DPCA for Negotiating Mission Critical QCIs

The following section provides the configuration commands to enable support for MC-PTT QCI feature.

Enabling Mission Critical QCI Feature

Use the following configuration commands to enable MC-PTT QCI feature.

```
configure
context context_name
  ims-auth-service service_name
  policy-control
    diameter encode-supported-features mission-critical-qcis
  end
```

Notes:

- **mission-critical-qcis**: This keyword enables MC-PTT QCI feature. By default, this feature will not be enabled.
- This keyword can be enabled only if the WPS license is configured. For more information, contact your Cisco account representative.
- To disable the negotiation of this feature, the existing **no diameter encode-supported-features** command needs to be configured. On executing this command, none of the configured supported features will be negotiated with PCRF.

Verifying the Mission Critical QCI Feature Configuration

The **show ims-authorization sessions full all** command generates a display that indicates the configuration status of this feature.

The following sample display is only a portion of the output which shows *mission-critical-qcis* among the Negotiated Supported Features.

```
show ims-authorization sessions full all

CallId: 00004e29          Service Name:  ims-ggsn-auth
IMSI: 123456789012341
....

Negotiated Supported Features:
3gpp-r8
mission-critical-qcis
Bound PCRF Server: 192.1.1.1
Primary PCRF Server: 192.1.1.1
Secondary PCRF Server: NA
....
```

Monitoring and Troubleshooting the Mission Critical QCI

The following section describes commands available to monitor the Mission Critical QCI feature.

Mission Critical QCI Show Command(s) and/or Outputs

```
show ims-authorization sessions full all
```

On running the above mentioned show command, statistics similar to the following are displayed and will indicate if the Mission Critical QCI feature is enabled or not.

```
show ims-authorization sessions full all

CallId: 00004e29           Service Name:  ims-ggsn-auth
IMSI: 123456789012341
....

Negotiated Supported Features:
3gpp-r8
mission-critical-qcis
....
```

HSS and PCRF-based P-CSCF Restoration Support for WLAN

This section describes the overview and implementation of the HSS-based and PCRF-based P-CSCF Restoration feature for WLAN and EPC networks.

This section includes the following topics:

- [Feature Description, on page 470](#)
- [Configuring the HSS/PCRF-based P-CSCF Restoration, on page 471](#)
- [Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration, on page 473](#)

Feature Description

The P-CSCF restoration procedures were standardized to minimize the time a UE is unreachable for terminating calls after a P-CSCF failure. In compliance with 3GPP standard Release 13, this feature is developed to include the following P-CSCF restoration mechanisms:

- HSS-based P-CSCF Restoration for Trusted/Untrusted WLAN Access (S2a/S2b)
- PCRF-based P-CSCF Restoration for LTE (S5/S8) and Trusted/Untrusted WLAN Access (S2a/S2b)



Important

HSS-based P-CSCF Restoration was supported at P-GW for LTE (S5/S8) prior to StarOS release 21.0.

This feature provides support for both basic and extended P-CSCF Restoration procedures.



Important

The P-CSCF Restoration is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

• HSS-based P-CSCF Restoration for WLAN:

If the P-CSCF restoration mechanism is supported, gateway indicates the restoration support to AAA server through Feature-List AVP in the Authorization Authentication Request (AAR) message sent over S6b interface. The Feature-List AVP is part of the Supported-Features grouped AVP. The Bit 0 of the Feature-List AVP is used to indicate P-CSCF Restoration support for WLAN.

During the P-CSCF Restoration, 3GPP AAA server, after having checked that the PGW supports the HSS-based P-CSCF restoration for WLAN, sends a P-CSCF restoration indication to the P-GW over

S6b in a Re-authorization Request (RAR) command. A new Diameter AVP “**RAR-Flags**” is encoded in the RAR message with the Bit 1 set, would indicate to the gateway that the AAA server requests the execution of HSS-based P-CSCF restoration procedures for WLAN.

The existing CLI command **diameter authentication** under AAA Group configuration is extended to encode P-CSCF Restoration feature as part of Supported-Features AVP in the AAR message.



Important

Supported-Features will be sent in every AAR message for RAT type WLAN. Feature negotiation is required in every AAR. ReAuth AAR will also do the feature renegotiation.

• PCRF-based P-CSCF Restoration:

PCEF supporting P-CSCF restoration mechanism indicates the restoration support in CCR-I message through the Supported-Features AVP. The 24th Bit of the Supported-Feature-List AVP indicates whether this mechanism is supported or not.

The existing CLI command **diameter encode-supported-features** in Policy Control configuration is extended to allow the negotiation of P-CSCF Restoration feature support with PCRF. A new Diameter AVP “**PCSCF-Restoration-Indication**” is introduced to indicate to PCEF that a P-CSCF Restoration is requested. This is achieved by setting AVP value to 0.

Supported-Features AVP is negotiated in CCR-I of all access types (eHRPD, P-GW, GGSN); however, Restoration trigger, if received, is ignored in eHRPD and GGSN.

Limitations

- As per the 3GPP standard specification, if S6b re-authorization request is used for P-CSCF Restoration for WLAN, then for extended P-CSCF Restoration the gateway may send authorization request with only mandatory AVPs. However, in the current implementation, ReAuth used for extended P-CSCF Restoration is a common authorization request of normal ReAuth. It will contain all the AVP of ReAuthorization AAR.

For more information on this feature and associated configurations, refer to *P-GW Enhancements for 21.0* and *SAEGW Enhancements for 21.0* section in the *Release Change Reference* guide.

Configuring the HSS/PCRF-based P-CSCF Restoration

The following section provides the configuration commands to enable support for HSS-based and PCRF-based P-CSCF Restoration feature.

Enabling P-CSCF Restoration Indication on S6b AAA interface

Use the following configuration commands for encoding Supported-Features AVP in the AAR message sent to AAA server via S6b interface.

configure

```
context context_name
  aaa group group_name
    diameter authentication encode-supported-features pscf-restoration-indication
  end
```

Notes:

- **encode-supported-features**: Encodes Supported-Features AVP.

- **pcscf-restoration-indication**: Enables the P-CSCF Restoration Indication feature.
- **default encode-supported-features**: Configures the default setting, that is not to send the Supported-Features AVP in AAR message.
- **no encode-supported-features**: Disables the CLI command to not send the Supported-Features AVP.
- The **pcscf-restoration-indication** keyword is license dependent. For more information, contact your Cisco account representative.

Enabling P-CSCF Restoration Indication on Gx interface

Use the following configuration to enable P-CSCF Restoration Indication feature on Gx interface.

```
configure
context context_name
ims-auth-service service_name
policy-control
diameter encode-supported-features pcscf-restoration-ind
end
```

Notes:

- **pcscf-restoration-ind**: Enables the P-CSCF Restoration Indication feature. This keyword is license dependent. For more information, contact your Cisco account representative. By default, this feature is disabled.
- **default encode-supported-features**: The default configuration is to remove/reset the supported features.
- **no encode-supported-features**: Removes the previously configured supported features.

Verifying the HSS/PCRF-based P-CSCF Restoration

show ims-authorization sessions full all

This command generates a display that indicates the negotiation status of this feature.

The following sample display is only a portion of the output which shows **pcscf-restoration-ind** among the Negotiated Supported Features.

```
show ims-authorization sessions full all

CallId: 00004e22          Service Name:  imsa-Gx
IMSI: 123456789012341
....
Negotiated Supported Features:
3gpp-r8
pcscf-restoration-ind
....
```

show aaa group all

This show command displays **pcscf-restoration-ind** as part of Supported-Features, if this feature is configured under AAA group.

```
show aaa group all
Group name:  default
Context:    local

Diameter config:
Authentication:
....
Supported-Features: pcscf-restoration-ind
....
```

Monitoring and Troubleshooting the HSS/PCRF-based P-CSCF Restoration

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed for troubleshooting any failure related to this feature:

- Verify if the feature is enabled using **show ims-authorization sessions full all** and **show aaa group all** CLI commands. If not enabled, configure the required CLI commands both under Policy Control and AAA group configuration and check if it works.
- Execute **monitor protocol** command and check if the support for P-CSCF Restoration feature is negotiated in CCR-I and AAR messages. If not, enable the respective CLI commands for this feature to work.
- If the failure is still observed, obtain the following information and contact Cisco account representative for further analysis:
 - Monitor protocol log with options 74 (EGTPC) and 75 (App Specific Diameter –Gx/S6b) turned on
 - Logs with sessmgr, imsa, and diameter-auth enabled
 - Output of **show session disconnect reason** CLI command and the relevant statistics at service level

Show Commands and/or Outputs

show ims-authorization sessions full all

The **Negotiated Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is negotiated with PCRF.

This supported feature is displayed only when the feature license is configured.

show aaa group all

The **Supported Features** field in this show command output displays whether or not the P-CSCF Restoration feature is configured as part of the Supported-Features AVP.

This supported feature is displayed only when the feature license is configured.

show license information

If the license to enable the P-CSCF Restoration feature is configured, then the **show license information** command displays the associated license information.

Monitoring Logs

This section provides information on how to monitor the logs that are generated relating to the HSS/PCRF-based P-CSCF Restoration feature.

S6b Diameter Protocol Logs

The **Supported-Features** field is available in AAR/AAA section. The log output generated will appear similar to the following:

```
<<<<OUTBOUND 15:37:23:561 Eventid:92870(5)
....
[V] [M] Supported-Features:
      [M] Vendor-Id: 10415
      [V] Feature-List-ID: 1
```

```

[V] Feature-List: 1
....
INBOUND>>>> 15:37:23:562 Eventid:92871(5)
....
[V] [M] Supported-Features:
[M] Vendor-Id: 10415
[V] Feature-List-ID: 1
[V] Feature-List: 1
....

```

The **RAR-Flags** field is available in RAR section. The log output generated will appear similar to the following:

```

INBOUND>>>> 15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....

```

Gx Diameter Protocol Logs

Under **Supported-Features**, the P-CSCF Restoration **Feature-List** is available in CCR-I/CCA-I section. The output generated will appear similar to the following:

```

<<<<OUTBOUND 13:52:06:117 Eventid:92820(5)
....
[V] [M] Supported-Features:
[M] Vendor-Id: 10415
[V] Feature-List-ID: 1
[V] Feature-List: 1677217
....
INBOUND>>>> 13:52:06:118 Eventid:92821(5)
....
[V] [M] Supported-Features:
[M] Vendor-Id: 10415
[V] Feature-List-ID: 1
[V] Feature-List: 1677216
....

```

The **PCSCF-Restoration-Indication** AVP is available in RAR. The output generated will appear similar to the following:

```

INBOUND>>>> 13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] PCSCF-Restoration-Indication: 0
....

```

Loop Prevention for Dynamic Rules

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	P-GW
Applicable Platform(s)	ASR 5500

Default Setting	Disabled
Related CDETS ID(s)	CSCvc97345, CSCvd02249
Related Changes in This Release	Not Applicable
Related Documentation	P-GW Administration Guide Command Line Interface Reference

Revision History



Important

Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When a PCC (Dynamic or Predefined) rule installation fails, the PCEF initiates a CCR-U toward the PCRF to report the failed rule. In case the PCRF responds back with same rule definition, then the rule failure CCR-U is initiated again. This results in a loop of rule failure.

With this feature, gateways have the ability to prevent the loop by reporting the rule install failure to PCRF only once until it is successfully installed.

How It Works

This feature is configurable through a CLI command with which, once a failure is being reported for a subscriber, failure for the same rule is suppressed for that subscriber until it is installed successfully. The rulenames are preserved for a subscriber for which the failures are reported. However, when the condition of the rule failure is rectified for an error (for example, rule definition is added to the configuration and the rule is successfully installed), then the gateway removes the rulename from the failed rules list. So, if the failure for that particular rule occurs again, it is reported to the PCRF.

The failed rulename is not checkpointed and so, if a recovery event like session recovery or an ICSR occurs then the failure of these rules are reported once again.

Configuring Loop Prevention for Dynamic Rules

This section explains the configuration procedures required to enable the feature.

Enabling ACS Policy to Control Loop Prevention

Use the following commands under ACS Configuration Mode to enable or disable the feature which prevents the rule failure loop between PCRF and PCEF:

```
configure
  active-charging service<service_name>
    policy-control report-rule-failure-once
  end
```

Notes:

- When configured, CCR-U will be sent only once for the same rule failure.
- By default, the feature is disabled.
- If previously configured, use the **no policy-control report-rule-failure-once** to disable the feature.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for the Loop Prevention for Dynamic Rules feature.

show active-charging service all

The output of the above command has been enhanced to display the status (Enabled/Disabled) of the feature. For example:

```
show active-charging service all
.
.
.
Report Rule Failure Once: Enabled
```

show active-charging subscribers full all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

Callid:	4e21	ACSMgr Card/Cpu:	15/0
Active Charging Service name:			acs
Active charging service scheme:			
ACSMgr Instance:	1	Number of Sub sessions:	1
Data Sessions Active:	0	Dynamic Routes created:	0
Uplink Bytes:	0	Downlink Bytes:	0
Uplink Packets:	0	Downlink Packets:	0
Accel Packets:	0		
FastPath Packets:	0		
Total NRSPCA Requests:	0	NRSPCA Req. Succeeded:	0
NRSPCA Req. Failed:	0		
Total NRUPC Requests:	0	NRUPC Req. Succeeded:	0
NRUPC Req. Failed:	0		
Pending NRSPCA Requests:	0	Pending NRUPC Requests:	0
Total Bound Dynamic Rules:	0	Total Bound Predef. Rules:	0
Data Sessions moved:	0		
Bearers Terminated for no rules:			0
Failed Rulebase Install (unknown bearer-id):			0


```
Failed Rule Install (unknown bearer-id): 0
Total number of rule failures not reported: 1
```

show active-charging subsystem all

The output of the above command has been enhanced to display the new parameter which shows the total number of rule failures not reported. For example:

```
Total ACS Managers:          2
Session Creation Succ:      1      Session Creation Fail:      0
.
.
.
Total Number of Unsolicited Downlink packets received : 0
Total Number of ICMP-HU packets sent :                  0

RADIUS Prepaid Statistics:
Total prepaid sess:          0      Current prepaid sess:      0
Total prepaid auth req:      0      Total prepaid auth success: 0
Total prepaid auth fail:      0      Total prepaid errors:      0
Total number of rule failures not reported :              4

Content Filtering URL Cache Statistics:
Total cached entries:        0
Total hits:                  0      Total misses:              0
.
.
.
```

Separation of Accounting Interim Interval Timer for RADIUS and Diameter Rf

Feature Information

Summary Data

Status	New Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	eHRPD, GGSN, P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CETS ID(s)	CSCvc97616
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference Command Line Interface Reference

Revision History



Important Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Prior to Release 21.2, the Cisco StarOS platform had a single configuration parameter for sending accounting interim records to RADIUS and Diameter Rf servers. Consequently, it was not possible to send accounting interim records to RADIUS and Diameter Rf servers with different intervals using the available CLI options. This feature provides a CLI controlled mechanism to have different interim intervals for Diameter Rf and RADIUS accounting applications. Having a separate configurable CLI and interim interval timer values for RADIUS and Diameter Rf servers provides enhanced usability.

How It Works

Currently, the Diameter accounting uses the value configured for RADIUS accounting interim interval. With this feature, configurable through a CLI command, provides an option to separately configure Diameter accounting interim interval for Rf interface. Until Diameter interim CLI is configured with either “**no**” option or any specific timer value, as a measure for compatibility, RADIUS interim interval value is used for Diameter interim interval. Once Diameter configuration takes effect, any change to RADIUS configuration will not affect Diameter configuration and vice versa. The following table shows the Diameter interim interval values used for different scenarios.

Radius Configuration	Diameter Configuration	Diameter Interim Behavior
No configuration OR Interim Interval: X OR Interim disabled	Interim Interval: Y	Interim Interval: Y Note: X may or may not be same as Y
No configuration OR Interim Interval: X OR Interim disabled	Interim disabled using “No” option	Interim disabled

Radius Configuration	Diameter Configuration	Diameter Interim Behavior
No configuration OR Interim Interval: X OR Interim disabled	No configuration	Fallback to RADIUS configuration

- Recovery/ICSR behavior: Interim interval configuration used at the time of PDN creation is applicable for entire lifetime of PDN. Recovery/ICSR will not have any impact of existing PDN behavior with regard to Diameter interim interval.
- ICSR Upgrade/Downgrade behavior:
 - Existing session will be recovered based on RADIUS configuration present in old chassis.
 - New session behavior is as per configuration available on newly active chassis.

Limitations

Following are the known limitations of this feature:

- 1 In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses the same interim interval value configured for RADIUS accounting.
- 2 Once diameter accounting configuration is done, it's not possible to go back to the older behavior.

Configuring Diameter Accounting Interim Interval

Use the following commands under AAA Server Group Configuration Mode to configure Diameter accounting interim interval independently from RADIUS accounting interim interval:

```
configure
context context_name
aaa group group_name
diameter accounting interim interval interval_in_seconds
end
```

Notes:

- *interval_in_seconds*: Specifies the interim interval, and must be in the range of 50 through 40000000.
- If previously configured, use the **no diameter accounting interim interval** to disable the interim accounting messages on Rf interface.
- There is no default Diameter interim interval value.
- In case Diameter interim interval CLI is not configured, the P-GW retains the older behavior where Diameter accounting uses RADIUS interim interval configuration available in AAA server group configuration block.

Monitoring and Troubleshooting

The following sections describe commands available to monitor the feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs in support of the feature.

show aaa group { name <group_name> | all }

The output of the above command is modified to display the following new field to show the current configuration for interim interval used for upcoming Diameter Rf accounting sessions:

- Interim-timeout: <50-40000000> or <None>

Following is a sample output where Diameter interim interval is not configured:

```
show aaa group name default
Group name:                default
Context:                   pgw

Diameter config:
  Accounting:
    Request-timeout:        20
    Interim-timeout:        None
```

Following is a sample output where Diameter interim interval is configured with the value 900:

```
show aaa group name default
Group name:                default
Context:                   pgw

Diameter config:
  Accounting:
    Request-timeout:        20
    Interim-timeout:        900
```

show configuration [verbose]

The output of the above command is modified to display the following new field to show the interval of interim messages in seconds:

- diameter accounting interim interval <value_in_seconds>

Following is a sample output where Diameter interim interval is configured with the value 60:

```
show configuration context isp verbose
config
  context isp
    aaa group default
      diameter accounting interim interval 60
```

Enhancement to OCS Failure Reporting for Gy

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Enabled
Related CDETS ID(s)	CSCvc93904
Related Changes in This Release	Not Applicable
Related Documentation	AAA Interface Administration and Reference P-GW Administration Guide SAEGW Administration Guide

Revision History



Important

Revision history details are not provided for features introduced before release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When Cisco-Event-Trigger-Type AVP is installed by PCRF in CCA-I, CCA-U or in RAR messages with value CREDIT_CONTROL_FAILURE (5), then the Cisco-Event grouped AVP is sent by the P-GW to PCRF in CCR-U message with the exact value of OCS failure code. This trigger is sent only when Gy failure occurs and based on the configuration (Credit-Control-Failure-Handling), the 'Continue' action is taken and Gy session moves to Offline state.

In releases prior to the implementation of this enhancement, if a failure code was received from OCS in the range of 3000-3999, then Cisco-CC-Failure-Type was sent with the value 3XXX. Similarly, for error codes in the range of 4000-4999 or 5000-5999, Cisco-CC-Failure-Type was reported as 4XXX or 5XXX respectively. With this enhancement, the exact failure code is reported to the PCRF instead of the range. For example, when the Cisco-Event-Trigger-Type is CREDIT_CONTROL_FAILURE (5) and OCS failure code is 3002 in CCA-U, then in CCR-U towards PCRF Cisco-CC-Failure-Type (as part of grouped AVP Cisco-Event) is sent with a value of 3002.

Support Added for RAN/NAS Cause Code for S5/S8 and S2b Interfaces

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.1
Modified-In Release(s)	21.2
Applicable Product(s)	P-GW, S-GW, SAEGW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCuy93748/CSCvc97356
Related Changes in This Release	Not Applicable
Related Documentation	<i>P-GW Administration Guide</i> <i>S-GW Administration Guide</i> <i>SAEGW Administration Guide</i> <i>Command Line Interface Reference</i>

Revision History



Important

Revision history details are not provided for features introduced before Release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Changes



Important

This is a license controlled feature. There are separate licenses for this feature. You must enable the existing license of NPLI or contact your Cisco account representative for information on how to obtain the custom license.

For billing co-ordination at IMS domain and VoWiFi deployments, an operator may require access to the RAN or NAS (or both) release cause code information available at P-CSCF. The P-GW provides detailed RAN/NAS cause information with ANI information received from the access network to the P-GW and further down to the PCRF based on the following events:

- Bearer deactivation (Delete Bearer Response/Delete Bearer Command)
- Session deactivation (Delete Session Request)
- Bearer creation/modification failures (Create/Update Bearer Response with cause as FAILURE)

The IMS network can retrieve detailed RAN and/or NAS release cause codes information from the access network that is used for call performance analysis, user QoE analysis, and proper billing reconciliation. This feature is supported on the S5, S8, Gx, and S2b interfaces.

This feature includes support RAN/NAS cause IE in Create Bearer Response, Update Bearer Response, Delete Bearer Response, Delete Bearer Command, and Delete Session Request. The following table shows the supported protocol type for RAN/NAS cause IE.

Table 34: Protocol Type for RAN/NAS IE

Interface	Supported Protocol Type for RAN/NAS IE
S5/S8	S1AP Cause (1)/EMM Cause (2)/ESM Cause (3)
S2b	Diameter Cause (4)/IKEv2 Cause (5)



Note

Any protocol type value that is received apart from the supported protocol type values listed in the table are ignored and not forwarded to the PCRF.

GTP interface Requirements for RAN/NAS Cause

For S5/S8 interface, RAN/NAS cause is supported for the following messages for the dpca-custom8 dictionary.

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request
- Delete Bearer Response
- Delete Bearer Command

For S2b interface, RAN/NAS cause is supported for the following messages for the custom dpca-custom8 dictionary:

- Failed Create Bearer Response
- Failed Update Bearer Response
- Delete Session Request

Gx interface Requirements for RAN/NAS Cause

The RAN/NAS cause is added for the custom dpca-custom8 dictionary to ensure that the RAN/NAS cause is populated. The Gx interface behavior to handle RAN/NAS cause is as follows:

Table 35: Gx Interface Requirements for RAN/NAS Cause

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Create Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.4-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U
Update Bearer Response	Accepted	RAN/NAS cause is not expected as per 29.274 Table 7.2.16-2. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	No Resources Available	CCR-U Note If UE-initiated (MBC) bearer modification fails with GTP cause "NO RESOURCES AVAILABLE", P-GW deletes the entire PDN session. In this case, RAN-NAS cause information is forwarded as part of CCR-T message.
	Context Not Found	CCR-U Note If the Update Bearer Response is received with the message level cause as "CONTEXT NOT FOUND", which leads to the PDN deletion, then the RAN-NAS cause information is forwarded as part of the CCR-T message.
	Temporarily rejected due to HO in progress.	RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.
	Other GTP Causes	CCR-U

Message	GTP Cause	Gx Message Carrying RAN-NAS Cause Information
Delete Bearer Response	Temporarily rejected due to HO in progress	<p>RAN/NAS cause with this GTP cause is not applicable as per 29.274 Table C.4. Therefore, if it is received, it is ignored and not forwarded to the PCRF.</p> <p>Note</p> <ul style="list-style-type: none"> • If RAN/NAS cause is received in the Delete Bearer Response, which is triggered as a part of the Delete Bearer command and cause as "Request Accepted", P-GW forwards the RAN/NAS cause (received in Delete Bearer Response) to the PCRF. • If RAN/NAS cause is received in the Delete Bearer command and Delete Bearer Response with HO in progress, the RAN/NAS Cause received in the Delete Bearer command is forwarded to the PCRF. • If RAN/NAS Cause is received in the Delete Bearer command and Delete Bearer Response with Accepted/Other Cause and new RAN/NAS Cause, the new RAN/NAS cause is forwarded to the PCRF.
	Accepted / Other GTP CCR-UCauses	<p>CCR-U</p> <p>Note If RAN/NAS cause is received in the delete bearer response that is initiated through RAR/CCA-U, then P-GW does not send CCR-U to the PCRF to report the RAN/NAS cause.</p> <p>This support is introduced in 29.212 release 13.5 with "Enhance RAN/NAS" feature".</p>
Delete Session Request	Accepted	CCR-T

ANI Behavior Towards PCRF

Section 4.5.6, 4.5.7, 4.5.12 of 3GPP 29.212 v13.4.0 mentions that if the RAN-NAS-Cause feature is supported, the PCEF should provide the available access network information within the 3GPP-User-Location-Info AVP (if available), TWAN-Identifier (if available and Trusted-WLAN feature is supported), User-Location-Info-Time AVP (if available), and 3GPP-MS-TimeZone AVP (if available).

In the earlier releases, the dpca-custom8 dictionary did not support USER-LOCATION-INFO-TIME AVP.

In this release, the USER-LOCATION-INFO-TIME AVP is added to the dpca-custom8 dictionary, which is sent to the PCRF (if available) as a part of ANI. Also, new PROTOCOL-TYPE, 1 to 5 are supported for RAN/NAS. This AVP can be seen in the CCR-U and CCR-T (whenever applicable). Also the new PROTOCOL-TYPE (S1AP Cause, EMM Cause, ESM Cause, IKEv2, DIAMETER) is visible on the Gx interface (if the same is received over the S5/S8/S2b interface).

ANI Behavior for S5/S8 Interface

Along with RAN/NAS cause, P-GW also sends following information to the PCRF, if available, for the dpca-custom8 dictionary:

Table 36: Mapping of GTP IE to ANI AVPs on Gx Interface

GTP IE	Gx AVP
UE Time Zone	3GPP-MS-TimeZone
ULI Timestamp	User-Location-Info-Time
User Location Information	3GPP-User-Location-Info

ANI information is sent to the PCRF irrespective of the event triggers configured when the RAN/NAS feature is enabled.

ANI Behavior for S2b Interface

ANI information is not sent towards PCRF for the dpca-custom8 dictionary. Also, the TWAN-Identifier is not supported as part of ANI for the dpca-custom8 dictionary.

Limitations

Following are the limitations of this feature:

- Support of RAN/NAS cause information is added only for the dpca-custom8 dictionary.
- PGW processes first two RAN/NAS cause IE (max one RAN and max one NAS) information received from the GTP interface. For example, if the access network misbehaves and sends RAN/NAS cause list with two NAS and one RAN then only first two causes are considered and validated. In this case, there are two NAS causes, only first NAS cause is populated at the Gx interface.
- RAN/NAS information is populated only on the Gx interface, no other interface is impacted.

Command Changes

diameter encode-supported-features netloc-ran-nas-cause

Use the existing CLI command, **diameter encode-supported-features netloc-ran-nas-cause** to enable the RAN/NAS cause on each of the S5/S8 and S2b interfaces.

This feature is disabled by default.

To enable this feature, enter the following commands:

```
configure
context ISP1
ims-auth-service MSGx
policy-control
diameter encode-supported-features netloc-ran-nas-cause
end
```



Gy Interface Support

This chapter provides an overview of the Gy interface and describes how to configure the Gy interface.

Gy interface support is available on the Cisco system running StarOS 9.0 or later releases for the following products:

- GGSN
- HA
- IPSG
- PDSN
- P-GW

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

- [Introduction, page 487](#)
- [Features and Terminology, page 489](#)
- [Configuring Gy Interface Support, page 529](#)

Introduction

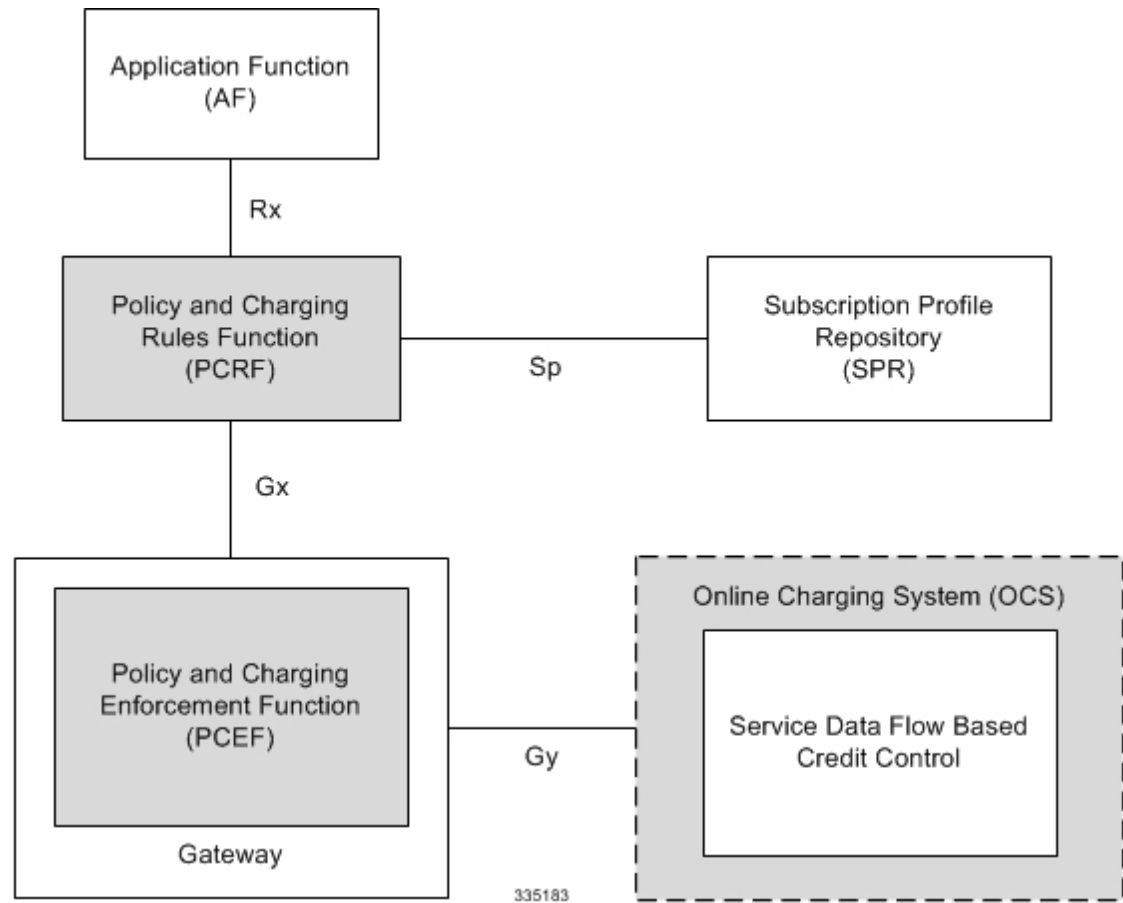
The Gy interface is the online charging interface between the PCEF/GW (Charging Trigger Function (CTF)) and the Online Charging System (Charging-Data-Function (CDF)).

The Gy interface makes use of the Active Charging Service (ACS) / Enhanced Charging Service (ECS) for real-time content-based charging of data services. It is based on the 3GPP standards and relies on quota allocation. The Online Charging System (OCS) is the Diameter Credit Control server, which provides the online charging data to the PCEF/GW. With Gy, customer traffic can be gated and billed in an online or prepaid style. Both time- and volume-based charging models are supported. In these models differentiated rates can be applied to different services based on ECS shallow- or deep-packet inspection.

In the simplest possible installation, the system will exchange Gy Diameter messages over Diameter TCP links between itself and one prepaid server. For a more robust installation, multiple servers would be used. These servers may optionally share or mirror a single quota database so as to support Gy session failover from

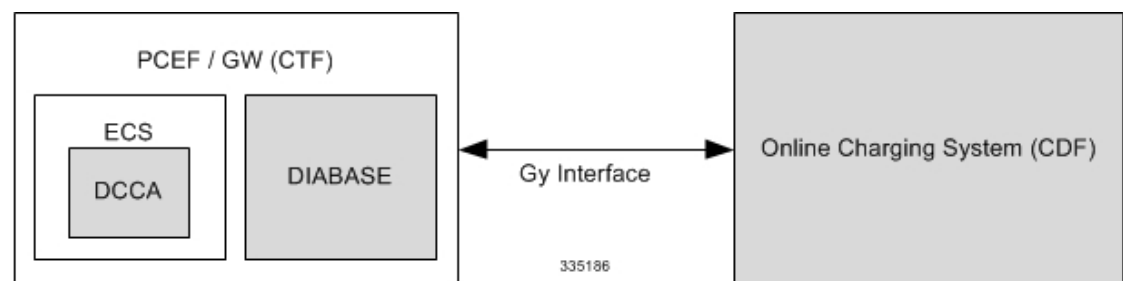
one server to the other. For a more scalable installation, a layer of proxies or other Diameter agents can be introduced to provide features such as multi-path message routing or message and session redirection features. The following figure shows the Gy reference point in the policy and charging architecture.

Figure 65: PCC Logical Architecture



The following figure shows the Gy interface between CTF/Gateway/PCEF/Client running ECS and OCS (CDF/Server). Within the PCEF/GW, the Gy protocol functionality is handled in the DCCA module (at the ECS).

Figure 66: Gy Architecture



License Requirements

The Gy interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Supported Standards

Gy interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)

Features and Terminology

This section describes features and terminology pertaining to Gy functionality.

Charging Scenarios



Important

Online charging for events ("Immediate Event Charging" and "Event Charging with Reservation") is not supported. Only "Session Charging with Reservation" is supported.

Session Charging with Reservation

Session Charging with Unit Reservation is used for credit control of sessions.

Decentralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the reservation of units prior to session supervision. An account debit operation is carried out following the conclusion of session termination.

Centralized Unit Determination and Centralized Rating

In this scenario, the CTF requests the OCS to reserve units based on the session identifiers specified by the CTF. An account debit operation is carried out following the conclusion of session.

Decentralized Unit Determination and Decentralized Rating



Important

Decentralized Rating is not supported in this release. Decentralized Unit determination is done using CLI configuration.

In this scenario, the CTF requests the OCS to assure the reservation of an amount of the specified number of monetary units from the subscriber's account. An account debit operation that triggers the deduction of the amount from the subscriber's account is carried out following the conclusion of session establishment.

Basic Operations



Important

Immediate Event Charging is not supported in this release. "Reserve Units Request" and "Reserve Units Response" are done for Session Charging and not for Event Charging.

Online credit control uses the basic logical operations "Debit Units" and "Reserve Units".

- Debit Units Request; sent from CTF to OCS: After receiving a service request from the subscriber, the CTF sends a Debit Units Request to the OCS. The CTF may either specify a service identifier (centralised unit determination) or the number of units requested (decentralised unit determination). For refund purpose, the CTF sends a Debit Units Request to the OCS as well.
- Debit Units Response; sent from OCS to CTF: The OCS replies with a Debit Units Response, which informs the CTF of the number of units granted as a result of the Debit Units Request. This includes the case where the number of units granted indicates the permission to render the requested service. For refund purpose, the OCS replies with a Debit Units Response.
- Reserve Units Request; sent from CTF to OCS: Request to reserve a number of units for the service to be provided by an CTF. In case of centralised unit determination, the CTF specifies a service identifier in the Reserve Unit Request, and the OCS determines the number of units requested. In case of decentralised unit determination, the number of units requested is specified by the CTF.
- Reserve Units Response; sent from OCS to CTF: Response from the OCS which informs the CTF of the number of units that were reserved as a result of the "Reserve Units Request".

Session Charging with Unit Reservation (SCUR) use both the "Debit Units" and "Reserve Units" operations. SCUR uses the Session Based Credit Control procedure specified in RFC 4006. In session charging with unit reservation, when the "Debit Units" and "Reserve Units" operations are both needed, they are combined in one message.



Important

Cost-Information, Remaining-Balance, and Low-Balance-Indication AVPs are not supported.

The consumed units are deducted from the subscriber's account after service delivery. Thus, the reserved and consumed units are not necessarily the same. Using this operation, it is also possible for the CTF to modify the current reservation, including the return of previously reserved units.

Re-authorization

The server may specify an idle timeout associated with a granted quota. Alternatively, the client may have a configurable default value. The expiry of that timer triggers a re-authorization request.

Mid-session service events (re-authorisation triggers) may affect the rating of the current service usage. The server may instruct the credit control client to re-authorize the quota upon a number of different session related triggers that can affect the rating conditions.

When a re-authorization is trigger, the client reports quota usage. The reason for the quota being reported is notified to the server.

Threshold based Re-authorization Triggers

The server may optionally include an indication to the client of the remaining quota threshold that triggers a quota re-authorization.

Termination Action

The server may specify to the client the behavior on consumption of the final granted units; this is known as termination action.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based. There are a series of message exchanges to check the status of the connection and the capabilities.

- Capabilities Exchange Messages: Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
 - Capabilities Exchange Request (CER): This message is sent from the client to the server to know the capabilities of the server.
 - Capabilities Exchange Answer (CEA): This message is sent from the server to the client in response to the CER message.



Important

Acct-Application-Id is not parsed and if sent will be ignored by the PCEF/GW. In case the Result-Code is not DIAMETER_SUCCESS, the connection to the peer is closed.

- Device Watchdog Request (DWR): After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable in PCEF/GW and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is taken to be down.

**Important**

DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- **Device Watchdog Answer (DWA):** This is the response to the DWR message from the server. This is used to monitor the connection state.
- **Disconnect Peer Request (DPR):** This message is sent to the peer to inform to shutdown the connection. PCEF/GW only receives this message. There is no capability currently to send the message to the diameter server.
- **Disconnect Peer Answer (DPA):** This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again. A timeout value for retrying the disconnected peer must be provided.
- **Tw Timer Expiry Behavior:** The connection between the client and the server is taken care by the DIABASE application. When two consecutive Tw timers are expired, the peer state is set to idle and the connection is retried to be established. All the active sessions on the connection are then transferred to the secondary connection if one is configured. All new session activations are also tried on the secondary connection.

There is a connection timeout interval, which is also equivalent to Tw timer, wherein after a CER has been sent to the server, if there is no response received while trying to reestablish connection, the connection is closed and the state set to idle.

Diameter Credit Control Application

The Diameter Credit Control Application (DCCA) is a part of the ECS subsystem. For every prepaid customer with Diameter Credit Control enabled, whenever a session comes up, the Diameter server is contacted and quota for the subscriber is fetched.

Quota Behavior

Various forms of quotas are present that can be used to charge the subscriber in an efficient way. Various quota mechanisms provide the end user with a variety of options to choose from and better handling of quotas for the service provider.

Time Quotas

The Credit-Control server can send the CC-Time quota for the subscriber during any of the interrogation of client with it. There are also various mechanisms as discussed below which can be used in conjunction with time quota to derive variety of methods for customer satisfaction.

- **Quota Consumption Time:** The server can optionally indicate to the client that the quota consumption must be stopped after a period equal to the "Quota Consumption Time" in which no packets are received or at session termination, whichever is sooner. The idle period equal to the Quota Consumption Time is included in the reported usage. The quota is consumed normally during gaps in traffic of duration less

than or equal to the Quota-Consumption-Time. Quota consumption resumes on receipt of a further packet belonging to the service data flow.

If packets are allowed to flow during a CCR (Update)/CCA exchange, and the Quota-Consumption-Time AVP value in the provided quota is the same as in the previously provided quota, then the Quota-Consumption-Time runs normally through this procedure. For example, if 5 seconds of a 10 second QCT timer have passed when a CCR(U) is triggered, and the CCA(U) returns 2 seconds later, then the QCT timer will expire 3 seconds after the receipt of the CCA and the remaining unaccounted 5 seconds of usage will be recorded against the new quota even though no packets were transmitted with the new quota.

A locally configurable default value in the client can be used if the server does not send the QCT in the CCA.

- **Combinational Quota:** Discrete-Time-Period (DTP) and Continuous-Time-Period (CTP) defines mechanisms that extends and generalize the Quota-Consumption-Time for consuming time-quota.
 - Both DTP and CTP uses a "base-time-interval" that is used to create time-envelopes of quota used.
 - Instead of consuming the quota linearly, DTP and CTP consumes the granted quota discretely in chunks of base-time-interval at the start of the each base-time-interval.
 - Selection of one of this algorithm is based on the "Time-Quota-Mechanism" AVP sent by the server in CCA.
 - Reporting usage can also be controlled by Envelope-Reporting AVP sent by the server in CCA during the quota grant. Based on the value of this AVP, the usage can be reported either as the usage per envelope or as usual cumulative usage for that grant.
- **Discrete-Time-Period:** The base-time-interval defines the length of the Discrete-Time-Period. So each time-envelope corresponds to exactly one Discrete-Time-Period. So when a traffic is detected, an envelope of size equal to Base-Time-Interval is created. The traffic is allowed to pass through the time-envelope. Once the traffic exceeds the base-time-interval another new envelope equal to the base-time-interval is created. This continues till the quota used exceeds the quota grant or reaches the threshold limit for that quota.
- **Continuous-Time-Period:** Continuous time period mechanism constructs time envelope out of consecutive base-time intervals in which the traffic occurred up to and including a base time interval which contains no traffic. Therefore the quota consumption continues within the time envelope, if there was traffic in the previous base time interval. After an envelope has closed, then the quota consumption resumes only on the first traffic following the closure of the envelope. The envelope for CTP includes the last base time interval which contains no traffic.

The size of the envelope is not constant as it was in Parking meter. The end of the envelope can only be determined retrospectively.

- **Quota Hold Time:** The server can specify an idle timeout associated with a granted quota using the Quota-Holding-Time AVP. If no traffic associated with the quota is observed for this time, the client understands that the traffic has stopped and the quota is returned to the server. The client starts the quota holding timer when quota consumption ceases. This is always when traffic ceases, i.e. the timer is re-started at the end of each packet. It applies equally to the granted time quota and to the granted volume quota. The timer is stopped on sending a CCR and re-initialized on receiving a CCA with the previous used value or a new value of Quota-Holding-Time if received.

Alternatively, if this AVP is not present, a locally configurable default value in the client is used. A Quota-Holding-Time value of zero indicates that this mechanism is not used.

- **Quota Validity Time:** The server can optionally send the validity time for the quota during the interrogation with the client. The Validity-Time AVP is present at the MSCC level and applies equally to the entire quota that is present in that category. The quota gets invalidated at the end of the validity time and a CCR-Update is sent to the server with the Used-Service-Units AVP and the reporting reason as VALIDITY_TIME. The entire quota present in that category will be invalidated upon Quota-Validity-Time expiry and traffic in that category will be passed or dropped depending on the configuration, till a CCA-Update is received with quota for that category.

Validity-Time of zero is invalid. Validity-Time is relative and not absolute.

In releases prior to 17.0, the AVP "SN-Remaining-Service-Unit" was not sent in the CCR-T and CCR-U messages with reporting Reason FINAL when the FUI action was received as Redirect and the granted units was zero in CCA. In 17.0 and later releases, for the Final-Reporting, the AVP "SN-Remaining-Service-Unit" will be encoded.

The "SN-Remaining-Service-Unit" AVP behavior is inherited from "Used-Service-Unit" AVP. This Final-Reporting is missing for the Remaining-Service-Unit AVP, which is now incorporated.

Volume Quota

The server sends the CC-Total-Octets AVP to provide volume quota to the subscriber. DCCA currently supports only CC-Total-Octets AVP, which applies equally to uplink and downlink packets. If the total of uplink and downlink packets exceeds the CC-Total-Octets granted, the quota is assumed to be exhausted.

If CC-Input-Octets and/or CC-Output-Octets is provided, the quota is counted against CC-Input-Octets and/or CC-Output-Octets respectively.



Important

Restricting usages based on CC-Input-Octets and CC-Output-Octets is not supported in this release.

Units Quota

The server can also send a CC-Service-Specific-Units quota which is used to have packets counted as units. The number of units per packet is a configurable option.

Granting Quota

Gy implementation assumes that whenever the CC-Total-Octets AVP is present, volume quota has been granted for both uplink and downlink.

If the Granted-Service-Unit contains no data, Gy treats it as an invalid CCA.

If the values are zero, it is assumed that no quota was granted.

If the AVP contains the sub AVPs without any data, it is assumed to be infinite quota.

Additional parameters relating to a category like QHT, QCT is set for the category after receiving a valid volume or time grant.

If a default quota is configured for the subscriber, and subscriber traffic is received it is counted against the default quota. The default quota is applicable only to the initial request and is not regranted during the course of the session. If subscriber disconnects and reconnects, the default quota will be applied again for the initial request.

Requesting Quota

Quotas for a particular category type can be requested using the Requested-Service-Unit AVP in the CCR. The MSCC is filled with the Rating-Group AVP which corresponds to the category of the traffic and Requested-Service-Unit (RSU) AVP without any data.

The Requested-Service-Unit can contain the CC AVPs used for requesting specific quantity of time or volume grant. Gy CLI can be used to request quota for a category type.

Alternatively quota can also be requested from the server preemptively for a particular category in CCR-I. When the server grants preemptive quota through the Credit control answer response, the quota will be used only when traffic is hit for that category. Quota can be preemptively requested from the Credit Control server from the CLI.

In 12.3 and earlier releases, when no pre-emptive quota request is present in CCR-I, on hitting server unreachable state for initial request, MSCC AVP with RSU is present in the CCR-I on server retries. Release 14.0 onwards, the MSCC AVP is skipped in the CCR-I on server retries. Corresponding quota usage will be reported in the next CCR-U (MSCC AVP with USU and RSU).

Reporting Quota

Quotas are reported to the server for number of reasons including:

- Threshold
- QHT Expiry
- Quota Exhaustion
- Rating Condition Change
- Forced Reauthorization
- Validity Time Expiry
- Final during Termination of Category Instance from Server

For the above cases except for QHT and Final, the Requested-Service-Unit AVP is present in the CCR.

Reporting Reason is present in CCR to let the server know the reason for the reporting of Quota. The Reporting-Reason AVP can be present either in MSCC level or at Used Service Unit (USU) level depending on whether the reason applies to all quotas or to single quota.

When one of these conditions is met, a CCR Update is sent to the server containing a Multiple-Services-Credit-Control AVP(s) indicating the reason for reporting usage in the Reporting-Reason and the appropriate value(s) for Trigger, where appropriate. Where a threshold was reached, the DCCA still has the amount of quota available to it defined by the threshold.

For all other reporting reasons the client discards any remaining quota and either discards future user traffic matching this category or allows user traffic to pass, or buffers traffic according to configuration.

For Reporting-Reason of Rating Condition Change, Gy requires the Trigger Type AVP to be present as part of the CCR to indicate which trigger event caused the reporting and re-authorization request.

For Reporting-Reason of end user service denied, this happens when a category is blacklisted by the credit control server, in this case a CCR-U is sent with used service unit even if the values as zero. When more quota is received from the server for that particular category, the blacklisting is removed.

If a default quota has been set for the subscriber then the usage from the default quota is deducted from the initial GSU received for the subscriber for the Rating Group or Rating Group and Service ID combination.

Default Quota Handling

- If default quota is set to 0, no data is passed/reported.
- If default quota is configured and default quota is not exhausted before OCS responds with quota, traffic is passed. Initial default quota used is counted against initial quota allocated. If quota allocated is less than the actual usage then actual usage is reported and additional quota is requested. If no additional quota is available then traffic is denied.
- If default quota is not exhausted before OCS responds with denial of quota, gateway blocks traffic after OCS response. Gateway will report usage on default quota even in this case in CCR-U (FINAL) or CCR-T.
- If default quota is consumed before OCS responds, if OCS is not declared dead (see definition in use case 1 above) then traffic is blocked until OCS responds.

Thresholds

The Gy client supports the following threshold types:

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

A threshold is always associated with a particular quota and a particular quota type. In the Multiple-Services-Credit-Control AVP, the Time-Quota-Threshold, Volume-Quota-Threshold, and Unit-Quota-Threshold are optional AVPs.

They are expressed as unsigned numbers and the units are seconds for time quota, octets for volume quota and units for service specific quota. Once the quota has reached its threshold, a request for more quotas is triggered toward the server. User traffic is still allowed to flow. There is no disruption of traffic as the user still has valid quota.

The Gy sends a CCR-U with a Multiple-Services-Credit-Control AVP containing usage reported in one or more User-Service-Unit AVPs, the Reporting-Reason set to THRESHOLD and the Requested-Service-Unit AVP without data.

When quota of more than one type has been assigned to a category, each with its own threshold, then the threshold is considered to be reached once one of the unit types has reached its threshold even if the other unit type has not been consumed.

When reporting volume quota, the DCCA always reports uplink and downlink separately using the CC-Input-Octets AVP and the CC-Output-Octets AVP, respectively.

On receipt of more quotas in the CCA the Gy discards any quota not yet consumed since sending the CCR. Thus the amount of quota now available for consumption is the new amount received less any quota that may have been consumed since last sending the CCR.

Conditions for Reauthorization of Quota

Quota is re-authorized/requested from the server in case of the following scenarios:

- Threshold is hit
- Quota is exhausted
- Validity time expiry
- Rating condition change:
 - Cellid change: Applicable only to GGSN and P-GW implementations.
 - LAC change: Applicable only to GGSN and P-GW implementations.
 - QoS change
 - RAT change
 - SGSN/Serving-Node change: Applicable only to GGSN and P-GW implementations.

Discarding or Allowing or Buffering Traffic to Flow

Whenever Gy is waiting for CCA from the server, there is a possibility of traffic for that particular traffic type to be encountered in the Gy. The behavior of what needs to be done to the packet is determined by the configuration. Based on the configuration, the traffic is either allowed to pass or discarded or buffered while waiting for CCA from the server.

This behavior applies to all interrogation of client with server in the following cases:

- No quota present for that particular category
- Validity timer expiry for that category
- Quota exhausted for that category
- Forced Reauthorization from the server

In addition to allowing or discarding user traffic, there is an option available in case of quota exhausted or no quota circumstances to buffer the traffic. This typically happens when the server has been requested for more quota, but a valid quota response has not been received from the server, in this case the user traffic is buffered and on reception of valid quota response from the server the buffered traffic is allowed to pass through.

Procedures for Consumption of Time Quota

- QCT is zero: When QCT is deactivated, the consumption is on a wall-clock basis. The consumption is continuous even if there is no packet flow.
- QCT is active: When QCT is present in the CCA or locally configured for the session, then the consumption of quota is started only at the time of first packet arrival. The quota is consumed normally till last packet arrival plus QCT time and is passed till the next packet arrival.

If the QCT value is changed during intermediate interrogations, then the new QCT comes into effect from the time the CCA is received. For instance, if the QCT is deactivated in the CCA, then quota consumptions resume normally even without any packet flow. Or if the QCT is activated from deactivation, then the quota consumption resume only after receiving the first packet after CCA.

- QHT is zero: When QHT is deactivated, the user holds the quota indefinitely in case there is no further usage (for volume quota and with QCT for time quota). QHT is active between the CCA and the next CCR.
- QHT is non-zero: When QHT is present in CCA or locally configured for the session, then after a idle time of QHT, the quota is returned to the server by sending a CCR-Update and reporting usage of the quota. On receipt of CCR-U, the server does not grant quota. QHT timer is stopped on sending the CCR and is restarted only if QHT is present in the CCA.

QHT timer is reset every time a packet arrives.

Envelope Reporting

The server may determine the need for additional detailed reports identifying start time and end times of specific activity in addition to the standard quota management. The server controls this by sending a CCA with Envelope-Reporting AVP with the appropriate values. The DCCA client, on receiving the command, will monitor for traffic for a period of time controlled by the Quota-Consumption-Time AVP and report each period as a single envelope for each Quota-Consumption-Time expiry where there was traffic. The server may request envelope reports for just time or time and volume. Reporting the quota back to the server, is controlled by Envelope AVP with Envelope-Start-Time and Envelope-End-Time along with usage information.

Credit Control Request

Credit Control Request (CCR) is the message that is sent from the client to the server to request quota and authorization. CCR is sent before the establishment of MIP session, and at the termination of the MIP session. It can be sent during service delivery to request more quotas.

- Credit Control Request - Initial (CCR-I)
- Credit Control Request - Update (CCR-U)
- Credit Control Request - Terminate (CCR-T)
- Credit Control Answer (CCA)
- Credit Control Answer - Initial (CCA-I)
- Credit Control Answer - Update (CCA-U)

If the MSCC AVP is missing in CCA-U it is treated as invalid CCA and the session is terminated.

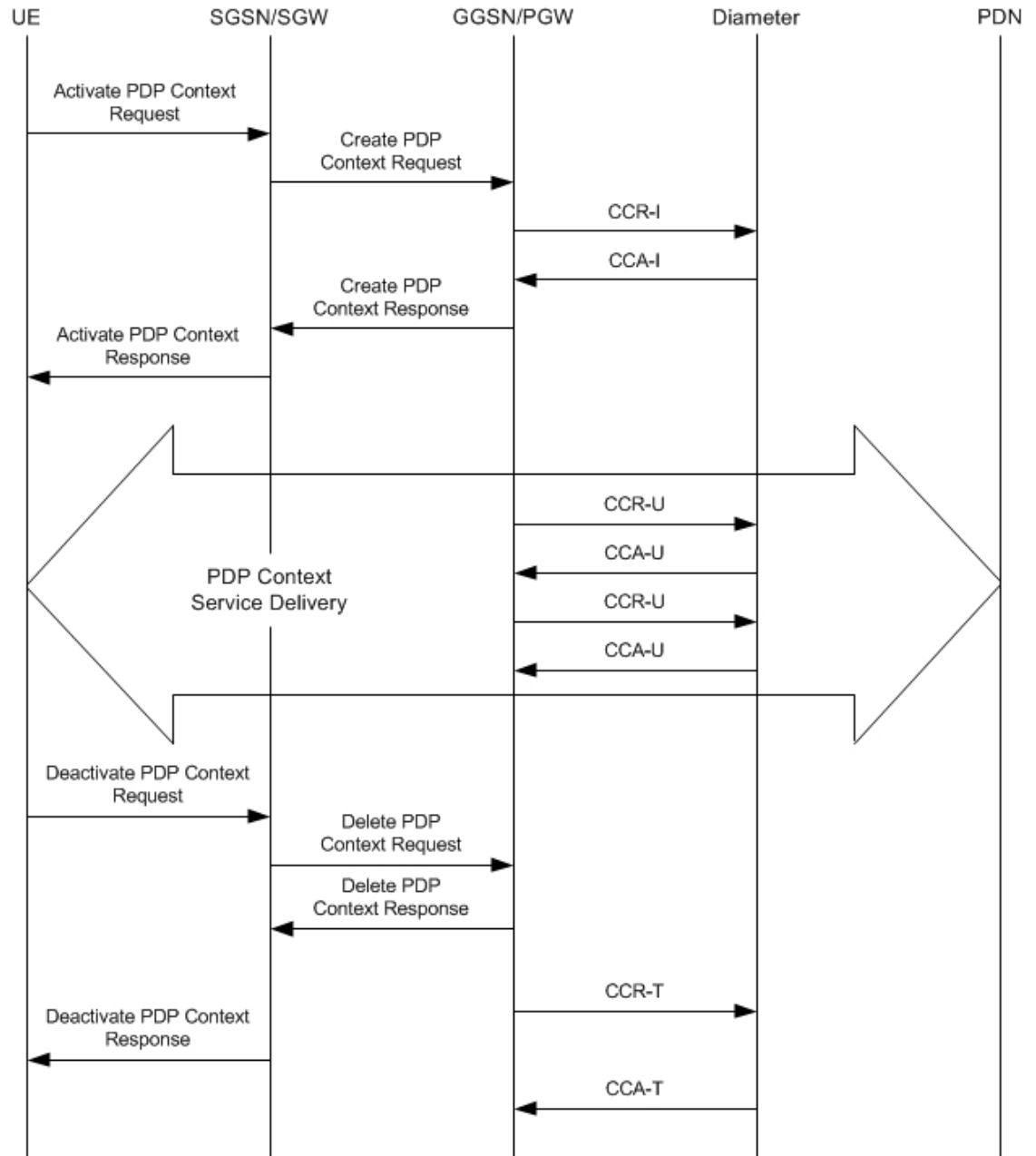
- Credit Control Answer - Terminate (CCA-T)

In releases prior to 16.0, CCR-T was immediately sent without waiting for CCA-U if the call was cleared and there was a pending CCA-U. In 16.0 and later releases, if call is cleared when there is a pending update, the gateway will wait for CCA-U to arrive or timeout to happen (whichever happens first).

In releases prior to 20, CCR-Ts were not reported over Gy interface when the calls were terminated due to audit failure during ICSR switchover. In 20 and later releases, DCCA allows generation of CCR-Ts in this scenario.

The following figure depicts the call flow for a simple call request in the GGSN/P-GW/IPSG Gy implementation.

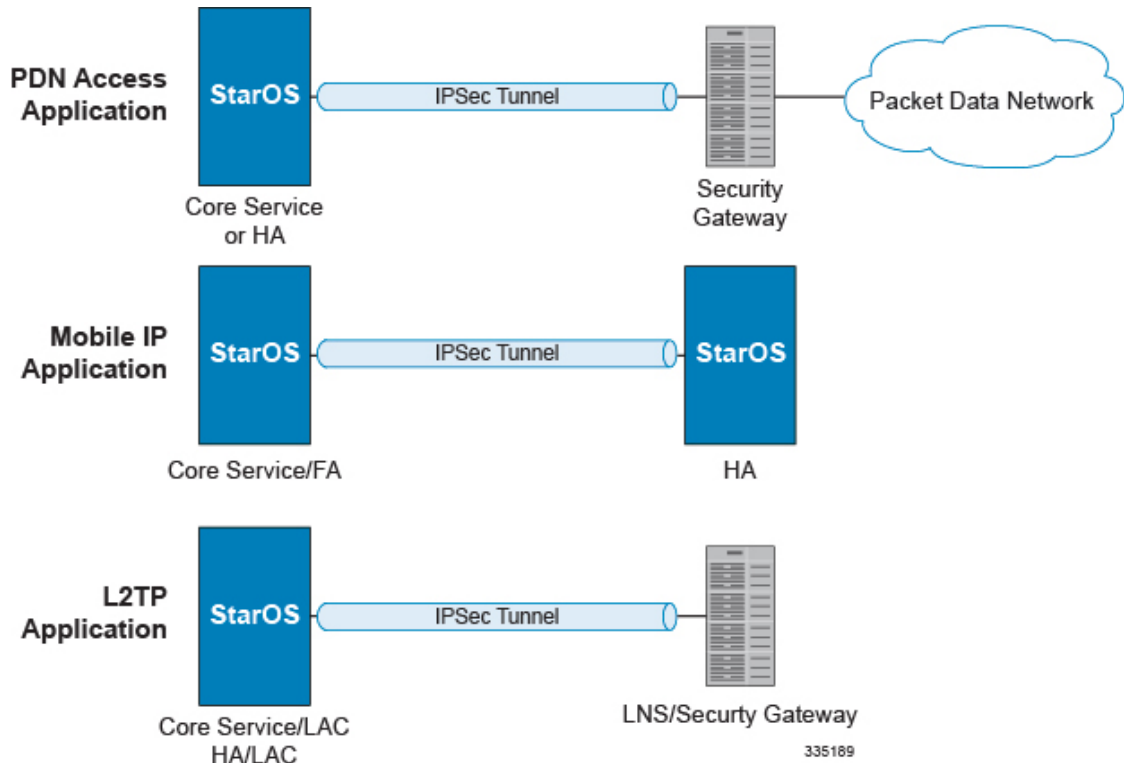
Figure 67: Gy Call Flow for Simple Call Request for GGSN/P-GW/IPSG



335187

The following figure depicts the call flow for a simple call request in the HA Gy implementation.

Figure 68: Gy Call Flow for Simple Call Request for HA



Tx Timer Expiry Behavior

A timer is started each time a CCR is sent out from the system, and the response has to arrive within Tx time. The timeout value is configurable in the Diameter Credit Control Configuration mode.

In case there is no response from the Diameter server for a particular CCR, within Tx time period, and if there is an alternate server configured, the CCR is sent to the alternate server after Tw expiry as described in "Tw Timer expiry behavior" section.

It also depends on the Credit-Control-Session-Failover AVP value for the earlier requests. If this AVP is present and is coded to FAILOVER_SUPPORTED then the credit-control message stream is moved to the secondary server, in case it is configured. If the AVP value is FAILOVER_NOT SUPPORTED, then the call is dropped in case of failures, even if a secondary server is configured.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U. In 16.0 and later releases, containers are closed only after CCA-U is received successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

Redirection

In the Final-Unit-Indication AVP, if the Final-Unit-Action is REDIRECT or Redirect-Server AVP is present at command level, redirection is performed.

The redirection takes place at the end of consumption of quota of the specified category. The Gy sends a CCR-Update without any RSU or Rating-Group AVP so that the server does not give any more quotas.

If the Final-Unit-Action AVP is RESTRICT_ACCESS, then according to the settings in Restriction-Filter-Rule AVP or Filter-Id AVP. Gy sends CCR-Update to the server with used quota.

Triggers

The Diameter server can provide with the triggers for which the client should reauthorize a particular category. The triggers can be configured locally as well but whatever trigger is present in the CCA from the server will have precedence.



Important

In this release, Gy triggers are not supported for HA.

The trigger types that are supported are:

- SGSN/Serving-Node Change
- QoS Change - Any
- RAT Change
- LAC Change
- CellID Change

On any event as described in the Trigger type happens, the client reauthorizes quota with the server. The reporting reason is set as RATING_CONDITION_CHANGE.

Tariff Time Change

The tariff change mechanism applies to each category instance active at the time of the tariff change whenever the server indicated it should apply for this category.

The concept of dual coupon is supported. Here the server grants two quotas, which is accompanied by a Tariff-Time-Change, in this case the first granted service unit is used until the tariff change time, once the tariff change time is reached the usage is reported up to the point and any additional usage is not accumulated, and then the second granted service unit is used.

If the server expects a tariff change to occur within the validity time of the quota it is granting, then it includes the Tariff-Time-Change AVP in the CCA. The DCCA report usage, which straddles the change time by sending two instances of the Used-Service-Unit AVP, one with Tariff-Change-Usage set to UNIT_BEFORE_TARIFF_CHANGE, and one with Tariff-Change-Usage set to UNIT_AFTER_TARIFF_CHANGE, and this independently of the type of units used by application. Both Volume and Time quota are reported in this way.

The Tariff time change functionality can as well be done using Validity-Time AVP, where in the Validity-Time is set to Tariff Time change and the client will reauthorize and get quota at Validity-Time expiry. This will trigger a lot of reauthorize request to the server at a particular time and hence is not advised.

Tariff-Time-Usage AVP along with the Tariff-Time-Change AVP in the answer message to the client indicates that the quotas defined in Multiple-Services-Credit-Control are to be used before or after the Tariff Time change. Two separate quotas are allocated one for before Tariff-Time-Change and one for after Tariff-Time-Change. This gives the flexibility to the operators to allocate different quotas to the users for different periods of time. In this case, the DCCA should not send the Before-Usage and After-Usage counts

in the update messages to the server. When Tariff-Time-Change AVP is present without Tariff-Time-Usage AVP in the answer message, then the quota is used as in single quota mechanism and the client has to send before usage and after usage quotas in the updates to the server.

**Important**

In this release, Gy does not support UNIT_INDETERMINATE value.

Final Unit Indication

The Final-Unit-Indication AVP can be present in the CCA from the server to indicate that the given quota is the final quota from the server and the corresponding action as specified in the AVP needs to be taken.

Final Unit Indication at Command Level

Gy currently does not support FUI AVP at command level. If this AVP is present at command level it is ignored. If the FUI AVP is present at command level and the Final-Unit-Action AVP set to TERMINATE, Gy sends a CCR-Terminate at the expiry of the quota, with all quotas in the USU AVP.

**Important**

FUI AVP at command level is only supported for Terminate action.

Final Unit Indication at MSCC Level

If the Final-Unit-Indication AVP is present at MSCC level, and if the Final-Unit-Action AVP is set to TERMINATE, a CCR-Update is sent at the expiry of the allotted quota and report the usage of the category that is terminated.

For information on redirection cases refer to the [Redirection](#), on page 500.

Credit Control Failure Handling

CCFH AVP defines what needs to be done in case of failure of any type between the client and the server. The CCFH functionality can be defined in configuration but if the CCFH AVP is present in the CCA, it takes precedence. CCFH AVP gives flexibility to have different failure handling.

Gy supports the following Failure Handling options:

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

CCFH with Failover Supported

In case there is a secondary server is configured and if the CC-Session-Failover AVP is set to FAILOVER_SUPPORTED, the following behavior takes place:

- Terminate: On any Tx expiry for the CCR-I the message is discarded and the session is torn down. In case of CCR-Updates and Terminates the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is torn down.

- **Continue:** On any Tx expiry, the message is sent to the secondary server after response timeout and the session is proceeded with the secondary server. In case there is a failure with the secondary server too, the session is still established, but without quota management.
- **Retry and Terminate:** On any Tx expiry, the message is sent to the secondary server after the response timeout. In case there is a failure with secondary server too, the session is taken down.

CCFH with Failover Not Supported

In case there is a secondary server configured and if the CC-Session-Failover AVP is set to `FAILOVER_NOT_SUPPORTED`, the following behavior takes place as listed below. Same is the case if there is no secondary server configured on the system.

- **Terminate:** On any Tx expiry, the session is taken down.
- **Continue:** On any Tx expiry, the session is still established, but without quota management.
- **Retry and Terminate:** On any Tx expiry, the session is taken down.

Failover Support

The CC-Session-Failover AVP and the Credit-Control-Failure-Handling (CCFH) AVP may be returned by the CC server in the CCA-I, and are used by the DCCA to manage the failover procedure. If they are present in the CCA they override the default values that are locally configured in the system.

If the CC-Session-Failover is set to `FAILOVER_NOT_SUPPORTED`, a CC session will never be moved to an alternative Diameter Server.

If the value of CC-Session-Failover is set to `FAILOVER_SUPPORTED`, then the Gy attempts to move the CC session to the alternative server when it considers a request to have failed, i.e:

- On receipt of result code "DIAMETER_UNABLE_TO_DELIVER", "DIAMETER_TOO_BUSY", or "DIAMETER_LOOP_DETECTED".
- On expiry of the request timeout.
- On expiry of Tw without receipt of DWA, if the server is connected directly to the client.

The CCFH determines the behavior of the client in fault situations. If the Tx timer expires then based on the CCFH value the following actions are taken:

- **CONTINUE:** Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). Note that quota management of other categories is not affected.
- **TERMINATE:** Terminate the MIP session, which affects all categories.
- **RETRY_AND_TERMINATE:** Allow the MIP session and user traffic for the relevant category or categories to continue, regardless of the interruption (delayed answer). The client retries to send the CCR when it determines a failure-to-send condition and if this also fails, the MIP session is then terminated.

After the failover action has been attempted, and if there is still a failure to send or temporary error, depending on the CCFH action, the following action is taken:

- **CONTINUE:** Allow the MIP session to continue.
- **TERMINATE:** Terminate the MIP session.

- **RETRY_AND_TERMINATE:** Terminate the MIP session.

Recovery Mechanisms

DCCA supports a recovery mechanism that is used to recover sessions without much loss of data in case of Session Manager failures. There is a constant check pointing of Gy data at regular intervals and at important events like update, etc.



Important

The DCCA supports maximum of three bearers (including default) for the ICSR Checkpointing and Recovery. When more than three bearers are configured in the DCCA, checkpointing occurs from Active to Standby for all the bearers. However, during recovery, only the first three bearers are recovered and the rest remain in the memory consuming resources.

For more information on recovery mechanisms, please refer to the *System Administration Guide*.

Error Mechanisms

Following are supported Error Mechanisms.

Unsupported AVPs

All unsupported AVPs from the server with "M" bit set are ignored.

Invalid Answer from Server

If there is an invalid answer from the server, Gy action is dependent on the CCFH setting:

- In case of continue, the MIP session context is continued without further control from Gy.
- In case of terminate and retry-and-terminate, the MIP session is terminated and a CCR-T is sent to the diameter server.

Result Code Behavior

- **DIAMETER_RATING_FAILED:** On reception of this code, Gy discards all traffic for that category and does not request any more quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_END_USER_SERVICE_DENIED:** On reception of this code, Gy temporarily blacklists the category and further traffic results in requesting new quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_CREDIT_LIMIT_REACHED:** On reception of this code, Gy discards all traffic for that category and waits for a configured time, after which if there is traffic for the same category requests quota from the server. This is supported at the MSCC level and not at the command level.
- **DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE:** On reception of this code, Gy allows the session to establish, but without quota management. This is supported only at the command level and not at the MSCC level.
- **DIAMETER_USER_UNKNOWN:** On reception of this code, DCCA does not allow the credit control session to get established, the session is terminated. This result code is supported only at the command level and not at the MSCC level.

For all other permanent/transient failures, Gy action is dependent on the CCFH setting.

Supported AVPs

The Gy functionality supports the following AVPs:

- Supported Diameter Credit Control AVPs specified in RFC 4006:
 - CC-Input-Octets (AVP Code: 412):
Gy supports this AVP only in USU.
 - CC-Output-Octets (AVP Code: 414):
Gy supports this AVP only in USU.
 - CC-Request-Number (AVP Code: 415)
 - CC-Request-Type (AVP Code: 416):
Gy currently does not support EVENT_REQUEST value.
 - CC-Service-Specific-Units (AVP Code: 417)
 - CC-Session-Failover (AVP Code: 418)
 - CC-Time (AVP Code: 420):
Gy does not support this AVP in RSU.
 - CC-Total-Octets (AVP Code: 421):
Gy does not support this AVP in RSU.
 - Credit-Control-Failure-Handling (AVP Code: 427)
 - Final-Unit-Action (AVP Code: 449):
Supported at Multiple-Services-Credit-Control grouped AVP level and not at command level.
 - Final-Unit-Indication (AVP Code: 430):
Fully supported at Multiple-Services-Credit-Control grouped AVP level and partially supported (TERMINATE) at command level.
 - Granted-Service-Unit (AVP Code: 431)
 - Multiple-Services-Credit-Control (AVP Code: 456)
 - Multiple-Services-Indicator (AVP Code: 455)
 - Rating-Group (AVP Code: 432)
 - Redirect-Address-Type (AVP Code: 433):
Gy currently supports only URL (2) value.
 - Redirect-Server (AVP Code: 434)
 - Redirect-Server-Address (AVP Code: 435)
 - Requested-Service-Unit (AVP Code: 437)
 - Result-Code (AVP Code: 268)

- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Subscription-Id (AVP Code: 443)
- Subscription-Id-Data (AVP Code: 444)
- Subscription-Id-Type (AVP Code: 450)
- Tariff-Change-Usage (AVP Code: 452):
Gy does NOT support UNIT_INDETERMINATE (2) value.
- Tariff-Time-Change (AVP Code: 451)
- Used-Service-Unit (AVP Code: 446):
Gy sends only incremental counts for all the AVPs from the last CCA-U.
- User-Equipment-Info (AVP Code: 458)
- User-Equipment-Info-Type (AVP Code: 459):
Gy currently supports only IMEISV value.
Cisco GGSN and P-GW support IMEISV by default.
- User-Equipment-Info-Value (AVP Code: 460)
- Validity-Time (AVP Code: 448)
- Supported 3GPP specific AVPs specified in 3GPP TS 32.299:
 - 3GPP-Charging-Characteristics (AVP Code: 13)
 - 3GPP-Charging-Id (AVP Code: 2)
 - 3GPP-GGSN-MCC-MNC (AVP Code: 9)
 - 3GPP-GPRS-QoS-Negotiated-Profile (AVP Code: 5)
 - 3GPP-IMSI-MCC-MNC (AVP Code: 8)
 - 3GPP-NSAPI (AVP Code: 10)
 - 3GPP-PDP-Type (AVP Code: 3)
 - 3GPP-RAT-Type (AVP Code: 21)
 - 3GPP-Selection-Mode (AVP Code: 12)
 - 3GPP-Session-Stop-Indicator (AVP Code: 11)
 - 3GPP-SGSN-MCC-MNC (AVP Code: 18)
 - 3GPP-User-Location-Info (AVP Code: 22)
 - Base-Time-Interval (AVP Code: 1265)
 - Charging-Rule-Base-Name (AVP Code: 1004)
 - Envelope (AVP Code: 1266)
 - Envelope-End-Time (AVP Code: 1267)

- Envelope-Reporting (AVP Code: 1268)
 - Envelope-Start-Time (AVP Code: 1269)
 - GGSN-Address (AVP Code: 847)
 - Offline-Charging (AVP Code: 1278)
 - PDP-Address (AVP Code: 1227)
 - PDP-Context-Type (AVP Code: 1247)
This AVP is present only in CCR-I.
 - PS-Information (AVP Code: 874)
 - Quota-Consumption-Time (AVP Code: 881):
This optional AVP is present only in CCA.
 - Quota-Holding-Time (AVP Code: 871):
This optional AVP is present only in the CCA command. It is contained in the Multiple-Services-Credit-Control AVP. It applies equally to the granted time quota and to the granted volume quota.
 - Reporting-Reason (AVP Code: 872):
Gy currently does not support the POOL_EXHAUSTED (8) value. It is used in case of credit-pooling which is currently not supported.
 - Service-Information (AVP Code: 873):
Only PS-Information is supported.
 - SGSN-Address (AVP Code: 1228)
 - Time-Quota-Mechanism (AVP Code: 1270):
The Gy server may include this AVP in an Multiple-Services-Credit-Control AVP when granting time quota.
 - Time-Quota-Threshold (AVP Code: 868)
 - Time-Quota-Type (AVP Code: 1271)
 - Trigger (AVP Code: 1264)
 - Trigger-Type (AVP Code: 870)
 - Unit-Quota-Threshold (AVP Code: 1226)
 - Volume-Quota-Threshold (AVP Code: 869)
- Supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
 - Auth-Application-Id (AVP Code: 258)
 - Destination-Host (AVP Code: 293)
 - Destination-Realm (AVP Code: 283)
 - Disconnect-Cause (AVP Code: 273)
 - Error-Message (AVP Code: 281)

- Event-Timestamp (AVP Code: 55)
- Failed-AVP (AVP Code: 279)
- Multiple-Services-Credit-Control (AVP Code: 456)
- Origin-Host (AVP Code: 264)
- Origin-Realm (AVP Code: 296)
- Origin-State-Id (AVP Code: 278)
- Redirect-Host (AVP Code: 292)
- Redirect-Host-Usage (AVP Code: 261)
- Redirect-Max-Cache-Time (AVP Code: 262)
- Rating-Group (AVP Code: 432)
- Result-Code (AVP Code: 268)
- Route-Record (AVP Code: 282)
- Session-Id (AVP Code: 263)
- Service-Context-Id (AVP Code: 461)
- Service-Identifier (AVP Code: 439)
- Supported-Vendor-Id (AVP Code: 265)
- Termination-Cause (AVP Code: 295)
- Used-Service-Unit (AVP Code: 446)
- User-Name (AVP Code: 1)

Unsupported AVPs

This section lists the AVPs that are NOT supported.

- NOT Supported Credit Control AVPs specified in RFC 4006:
 - CC-Correlation-Id
 - CC-Money
 - CC-Sub-Session-Id
 - CC-Unit-Type (AVP Code: 454)
 - Check-Balance-Result
 - Cost-Information (AVP Code: 423)
 - Cost-Unit (AVP Code: 445)
 - Credit-Control
 - Currency-Code (AVP Code: 425)
 - Direct-Debiting-Failure-Handling (AVP Code: 428)

- Exponent (AVP Code: 429)
- G-S-U-Pool-Identifier (AVP Code: 453)
- G-S-U-Pool-Reference (AVP Code: 457)
- Requested-Action (AVP Code: 436)
- Service-Parameter-Info (AVP Code: 440)
- Service-Parameter-Type (AVP Code: 441)
- Service-Parameter-Value (AVP Code: 442)
- Unit-Value (AVP Code: 424)
- Value-Digits (AVP Code: 447)
- NOT supported Diameter AVPs specified in 3GPP TS 32.299 V8.1.0:
 - Acct-Application-Id (AVP Code: 259)
 - Error-Reporting-Host (AVP Code: 294)
 - Experimental-Result (AVP Code: 297)
 - Experimental-Result-Code (AVP Code: 298)
 - Proxy-Host
 - Proxy-Info
 - Proxy-State
- NOT supported 3GPP-specific AVPs specified in 3GPP TS 32.299 V8.1.0:
 - 3GPP-CAMEL-Charging-Info (AVP Code: 24)
 - 3GPP-MS-TimeZone (AVP Code: 23)
 - 3GPP-PDSN-MCC-MNC
 - Authorised-QoS
 - Access-Network-Information
 - Adaptations
 - Additional-Content-Information
 - Additional-Type-Information
 - Address-Data
 - Address-Domain
 - Addressee-Type
 - Address-Type
 - AF-Correlation-Information
 - Alternate-Charged-Party-Address
 - Application-provided-Called-Party-Address

- Application-Server
- Application-Server-Information
- Applic-ID
- Associated-URI
- Aux-Applic-Info
- Bearer-Service
- Called-Asserted-Identity
- Called-Party-Address
- Calling-Party-Address
- Cause-Code
- Charged-Party
- Class-Identifier
- Content-Class
- Content-Disposition
- Content-Length
- Content-Size
- Content-Type
- Data-Coding-Scheme
- Deferred-Location-Event-Type
- Delivery-Report-Requested
- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- Event
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier (ICID)
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID

- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- Message-ID
- Message-Size
- Message-Type
- MMBBox-Storage-Requested
- MM-Content-Type
- MMS-Information

- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initiation-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- Priority
- PS-Append-Free-Format-Data (AVP Code: 867):
The PCEF/GW ignores this AVP if no PS free format data is stored for the online charging session.
- PS-Free-Format-Data (AVP Code: 866)
- PS-Furnish-Charging-Information (AVP Code: 865)
- RAI (AVP Code: 909)

- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance
- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data
- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp
- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node

- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange
- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI
- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

PLMN and Time Zone Reporting

For some implementations of online charging, the OCS requires the PCEF to reporting location-specific subscriber information. For certain subscriber types, subscriber information such as PLMN, Time Zone, and ULI can be sent over the Gy interface as the subscriber changes location, time zone, and serving networks to provide accurate online charging services. Such information can be reported independently from time and volume-based reporting.

PLMN and Time Zone Reporting feature is enabled to support location event reporting based on triggers from Gx, when the following conditions are met:

- Session-based Gy is not initiated due to the absence of charging-actions in rulebase with Credit-Control enabled or due to delayed Gy session initiation.
- PLMN and Time Zone Reporting feature is either enabled in the credit control group or through the use of triggers received from Gx.

If session-based Gy initiation fails or the session goes offline due to configuration or network issues, event-based Gy session will not be initiated.

**Important**

Note that the failure-handling will not be supported for event-based Gy.

Though, in event-based Gy, multiple events can be reported independently and simultaneously this is presently not supported. If an event occurs when the CCA-Event (CCA-E) of the previously reported event is awaited, then the new event is queued and reported only when a CCA-E is received or the message is timed out.

To enable the PLMN and Time Zone Reporting feature, the PCRF shall send the Trigger AVP (Trigger Type 1, Trigger Type 2) at the command level in a CCA.

The Event-based Gy session will be terminated in the following scenarios:

- On termination of the bearer/subscriber (subscriber level Gy).
- Initiation of session-based Gy session (delayed session initiation).
- Once the CCR-E transaction is complete and there are no further events to report.

For information on how to configure this feature, refer to the *Gy Interface Support* chapter in the administration guide for the product that uses the Gy interface functionality.

Interworking between Session-based Gy and Event-based Gy

If both session-based Gy and event-based Gy mode are activated, then session-based Gy will take precedence i.e. all the events will be reported through CCR-U if the corresponding triggers are enabled. Event-based Gy mode will be active only when session-based Gy has been disabled and has never been activated previously for this session during its lifetime.

OCS Unreachable Failure Handling Feature

The OCS Unreachable Failure Handling feature is required to handle when OCS goes down or unavailable. This feature is otherwise noted as Assume Positive for Gy.

The OCS is considered unavailable/unreachable in the following scenarios:

- PCEF transmits a CCR-U or CCR-I message but no response is received before the specified timeout
- Diameter Watchdog request times out to the current RDR, causing the TCP connection state to be marked down
- Diameter command-level error codes received in a CCA
- If the PCEF is unable to successfully verify transmission of a CCR-T, the PCEF will not assign interim quota, because the user has disconnected.

In 15.0 and later releases, the error result codes can be configured using the CLI command **servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }** to trigger the server unreachable mode. The same is applicable for the update request also. For more information on the CLI command, see the *Credit Control Configuration Mode Commands* chapter of the *Command Line Interface Reference*. However, if the CLI command **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [to end-result-code] }** is configured, then the default set of hard-coded error codes are applicable.

The default set is:

- UNABLE_TO_DELIVER 3002
- UNABLE_TOO_BUSY 3004
- LOOP_DETECTED 3005
- ELECTION_LOST 4003
- Permanent failures 5001-5999 except 5002, 5003 and 5031.

In 12.2 and later releases, existing failure handling mechanism is enhanced such that the subscriber can be allowed to browse for a pre-configured amount of interim-volume and/or interim-time if OCS becomes unreachable due to transport connection failure or gives an impression that OCS is unreachable owing to slow response for Diameter request messages.

The purpose of this feature is to support Gy based data sessions in the event of an OCS outage. Diameter client allows the user's data session to continue for some fixed quota and then retries the OCS server to restore normal functionality. This feature adds more granularity to the existing failure handling mechanism.

With the implementation of this feature, Gy reporting during outages is supported. A temporary time and/or volume quota is assigned to the user in the event of an OCS outage which will be used during the outage period.

When the OCS returns to service, the GW reports all used quota back to OCS and continues with normal Gy reporting.

For each DCCA-service, CLI control is available for the following options:

- Interim quota volume (in bytes) and quota time (seconds). Both values will apply simultaneously, if configured together and if either quota time or quota volume is exhausted, the Diameter client retries the OCS.
- Option to limit the number of times a session can be assigned a temporary quota. If the user exceeds this amount, the session will be terminated/converted to postpaid.

The quota value is part of the dcca-service configuration, and will apply to all subscribers using that dcca-service. The temporary quota will be specified in volume (bytes) and/or time (seconds) to allow enforcement of both quota tracking mechanisms individually or simultaneously.

When a user consumes the interim total quota or time configured for use during failure handling scenarios, the GW retries the OCS server to determine if functionality has been restored. In the event that services have been restored, quota assignment and tracking will proceed as per standard usage reporting procedures. Data used during the outage will be reported to the OCS.

In the event that the OCS services have not been restored, the GW re-allocates the configured amount of quota and/or time to the user. The GW reports all accumulated used data back to OCS when OCS is back online. If multiple retries and interim allocations occur, the GW reports quota used during all allocation intervals. This cycle will continue until OCS services have been successfully restored, or the maximum number of quota assignments has been exhausted.

Support for OCS unreachable CLI commands is added under Diameter Credit Control Configuration mode.

For the P-GW/XGW/GGSN, this behavior will apply to all APNs and subscribers that have online charging enabled by the PCRF. In the HA, this behavior will apply to all users that have online charging enabled by the AAA. Settings will be applied to the dcca-service.

In Release 15.0, the following enhancements are implemented as part of the Assume Positive Gy feature:

- Configurable per error code treatment to enter assume positive mode

- Graceful session restart upon receipt of a 5002 error

**Important**

Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Configurable per Error Code Treatment

This feature allows the customers to configure error result codes using the CLI command "**servers-unreachable behavior-triggers**" that will trigger entering assume positive mode on the fly for CCR-Initial and CCR-Update messages. CCR-Terminate message is currently not supported.

Any error result codes from the range 3xxx to 5xxx can be specified using the CLI commands. This feature has been implemented to provide more flexibility and granularity in the way assume positive mode is triggered for error result codes.

Graceful Session Restart

Graceful session restart upon receipt of a 5002 error code is supported for server retried CCR-U messages during assume positive state. Also, any unreported usage from the time, server retried CCR-U sent till CCA-I is received, will be reported immediately by triggering CCR-U with usages for the same.

**Important**

Note that the Graceful session restart feature is customer specific. For more information contact your Cisco account representative.

Any pending updates are aborted once CCA-U with 5002 is received from the server. Also CCR-U is triggered immediately following session restart only if there are any unreported usages pending.

**Important**

When the server responds with 5002 error result code, it does not include any granted service units for the requested rating groups.

For more information on the commands introduced in support of this feature, see the *Credit Control Configuration Mode Command* chapter in the *Command Line Interface Reference*.

Enhancement to OCS Failure Reporting for Gy

Feature Description

When Cisco-Event-Trigger-Type AVP is installed by PCRF in CCA-I, CCA-U or in RAR messages with value CREDIT_CONTROL_FAILURE (5), then the Cisco-Event grouped AVP is sent by the P-GW to PCRF in CCR-U message with the exact value of OCS failure code. This trigger is sent only when Gy failure occurs and based on the configuration (Credit-Control-Failure-Handling), the 'Continue' action is taken and Gy session moves to Offline state.

In releases prior to the implementation of this enhancement, if a failure code was received from OCS in the range of 3000-3999, then Cisco-CC-Failure-Type was sent with the value 3XXX. Similarly, for error codes in the range of 4000-4999 or 5000-5999, Cisco-CC-Failure-Type was reported as 4XXX or 5XXX respectively. With this enhancement, the exact failure code is reported to the PCRF instead of the range. For example, when

the Cisco-Event-Trigger-Type is CREDIT_CONTROL_FAILURE (5) and OCS failure code is 3002 in CCA-U, then in CCR-U towards PCRF Cisco-CC-Failure-Type (as part of grouped AVP Cisco-Event) is sent with a value of 3002.

Backpressure Handling

Diameter base (Diabase) maintains an outbound stream. When an application wants to write a message into a socket, the message handle of those messages are stored in the outbound stream. Only on receiving the response to the corresponding request, the stored message handle is removed from the outbound stream. In order to rate-limit the message transactions based on the responses received from the server, ASR 5500 maintains a limit on the number of messages stored in the outbound stream. This is done using "max-outstanding <>" CLI (default value is 256). If the number of messages created by the application exceeds the max-outstanding limit, diabase sends a 'Backpressure' indication to the application to wait till it receives a decongestion indication from diabase to try again.

On receiving a response from the server, the corresponding request message handle will be removed from the outbound stream, creating a slot for another message to be written by the application. In order to intimate this slot availability, decongestion notification is sent to the registered application. The application in turn loops through all sessions and processes the pending trigger to be sent.

When the application loops through the sessions in the system, it traverse the sessions in a sorted order and checks each session whether it has to send a pending CCR-Initial or CCR-Terminate or CCR-Update. When the first session gets the slot to fill the outbound stream, it writes the message into the stream. Now the slot gets back into filled state, reaching the max-outstanding limit again. So the rest of the sessions will still continue to be in backpressured state.

Backpressured request like Credit-Control-Initial and Credit-Control-Terminate are given higher priority over Credit-Control-Update as they are concerned with the creation or termination of a session. So on top of the decongestion notification, DCCA has some internal timers which periodically try to send the message out. So in case of heavy backpressure condition, the probability of CCR-I or CCR-T being sent out is more than CCR-U.

Gy Backpressure Enhancement

This feature facilitates maintaining a list of DCCA sessions that hit backpressure while creating a message i.e., backpressured list, eliminating the current polling procedure. This will maintain a single queue for all types of messages (CCR-I, CCR-U, CCR-T, CCR-E) that are backpressured. The messages will be sent in FIFO order from the queue.

After processing a session from the backpressure queue DCCA will check for the congestion status of the peer and continue only if the peer has empty slots in the outstanding message queue to accommodate further CCRs.

Releases prior to 16.0, the gateway has a max-outstanding configuration to manage a number of messages that are waiting for response from OCS. When the max-outstanding is configured to a low value, then the frequency to be in congested state is very high.

CPU utilization is very high if the max-outstanding count is low and network is congested.

In 16.0 and later releases, all DCCA sessions associated with the CCR messages that are triggered BACKPRESSURE (when max-outstanding has been reached) will be queued in backpressure list which is maintained per ACS manager instance (credit-control) level.

This list will not have any specific configurable limits on the number of sessions that will be queued in it. This is because there is an inherent limit that is already present which is dependent on the number of subscriber/DCCA sessions.

With this new separate backpressured list, CPU utilization will come down under high backpressure case.

Gy Support for GTP based S2a/S2b

For WiFi integration in P-GW, Gy support is provided for GTP based S2a/S2b in Release 18.0. This implementation is in compliance with standard Rel-11 non-3GPP access spec of 32.399: S5-120748 S5-131017 S5-143090.

As part of this enhancement, the following AVP changes are introduced:

- Added TWAN as a new enum value for Serving-Node-Type AVP
- Added a new Diameter AVP "TWAN-User-Location-Info". This is a grouped AVP and it contains the UE location in a Trusted WLAN Access Network (TWAN): BSSID and SSID of the access point.

The TWAN AVPs will be effective only for 3GPP release 11 and it is added only to the standard Gy dictionary. That is, the TWAN AVP will be included in CCR-I/CCR-U/CCR-T messages only when the CLI command "**diameter update-dictionary-avps 3gpp-rel11**" is configured.

Generating OOC/ROC with Changing Association between Rule and RG

The existing Gy implementation prevents duplicate Out-of-Credit (OOC) / Reallocation of Credit (ROC) report for the same rule to the PCRF. Subscriber throttling with the same rule with different Rating-Group across OOC event does not work. To overcome this, the following implementation is considered:

When a Rating-Group runs out of credit, OOC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already OOC'd or not. Similarly, when a Rating-Group gets quota after being in OOC state, a ROC is sent to all rules that are currently associated with that Rating-Group. This is done irrespective of whether that rule was already ROC'd or not.

In releases prior to 18, MSCC's state was previously being maintained at MSCC and rule-level to suppress OOC/ROC events. So if MSCC triggered an OOC/ROC the same was suppressed by the status maintained at the rule-level if the previous event on the rule was the same.

In 18 and later releases, the rule level status bits are no longer used to avoid similar back-to-back OOC/ROC events. Now, the triggering of OOC/ROC events will solely be dependent on the MSCC state and triggers.

Customers might see an increase in OOC/ROC events on Gx if they change the association of the rule and RG or if they use the Override feature.

Static Rulebase for CCR

An APN/subscriber can have a single rulebase applied to it, but allowing a static rulebase configuration to always pass a different or same rulebase to the OCS through CCR messages.

A new CLI command "**charging-rulebase-name rulebase_name**" has been introduced under Credit Control (CC) group to override/change the rulebase name present in APN/subscriber template, in the CCR AVP "Charging-Rule-Base-Name". The rulebase value configured in CC group will be sent to OCS via CCR. If

this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

This feature, when activated with the CLI command, reduces the complication involved in configuration of services like adding and removing services per enterprise on the OCS system.

CC based Selective Gy Session Control

This section describes the overview and implementation of the Selective Gy Session Control feature based on Charging Characteristics (CC) profile of the subscriber.

This section discusses the following topics for this feature:

- [Feature Description, on page 520](#)
- [Configuring CC based Selective Gy Session Control, on page 521](#)
- [Monitoring and Troubleshooting the Selective Gy Session Control Feature, on page 522](#)

Feature Description

The functionality that allows users to configure certain Charging Characteristics (CC) values as prepaid/postpaid is available for GGSN service. In Release 17, this functionality is extended to P-GW service.

To enable/disable Gy session based on the CC value received, the APN configuration is extended so that additional credit-control-groups/prepaid prohibited value can be configured for each of the CC values.

The **cc profile cc-profile-index prepaid prohibited** CLI command is used to configure the CC values to disable Credit-Control based charging. The P-GW/GGSN/SAEGW service subscriber sessions using this APN, can use this configuration to stop the triggering of Gy messages towards the OCS.

The UE provides the charging characteristics value and the active subscriber is connected through an APN. The CC index mapping is done for a corresponding CC group/prepaid prohibited value configured under the APN. Depending on the match, the Gy session is enabled or disabled towards the OCS.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging characteristic is selected and used. If there is no matching charging characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

When a particular CC is configured as postpaid, any session with this CC does not trigger Gy connection. Any change in the CC during the lifetime of session is ignored.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

Relationships to Other Features

This feature can also be used when the CC profile configuration is enabled through the GGSN service. When the CC profile is configured under APN service and GGSN service, the prepaid prohibited configuration for the matching CC profile is applied irrespective of the services.

Limitations

The following are the limitations of this feature:

- One charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.
- The charging-characteristic based OCS selection is possible only during the session-setup. Once the credit-control-group is selected (after session setup), this feature is not applicable.

Configuring CC based Selective Gy Session Control

The following sections provide the configuration commands to configure the Gy Session Control feature based on the CC profile of the subscriber.

Configuring CC Value

The following commands are used to configure Charging Characteristic values as postpaid/prepaid to disable/enable Gy session towards the OCS.

```
configure
context context_name
  apn apn_name
    cc-profile { cc_profile_index | any } { prepaid-prohibited | credit-control-group cc_group_name }
  end
```

Notes:

- *cc_profile_index*: Specifies the CC profile index. *cc_profile_index* must be an integer from 0 through 15.
- **any**: This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring **any** keyword will not override other specific configurations under APN.
- **prepaid-prohibited**: Disables prepaid Gy session for the configured profile index.
- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.
- **no cc-profile cc_profile_index**: This command falls back to "any" cc-profile behavior irrespective of the CC profile index value configured.

Verifying the Selective Gy Session Control Configuration

Use the following command in Exec mode to display/verify the configuration of Selective Gy Session Control feature.

show configuration

Monitoring and Troubleshooting the Selective Gy Session Control Feature

This section provides information regarding show commands and/or their outputs in support of the Selective Gy Session Control feature.

show active-charging sessions

The "Credit-Control" field that appears as part of the **show active-charging sessions [callid | imsi | msisdn]** command output enables the user to determine the credit control state as "On" for online charging enabled session or "Off" for prepaid prohibited session and monitor the subscriber session.

Credit-Control Group in Rulebase Configuration

This section describes the overview and implementation of the Credit-Control (CC) Group Selection based on the rulebase of the subscriber.

This section discusses the following topics for this feature:

- [Feature Description, on page 522](#)
- [Configuring Credit-Control Group in Rulebase, on page 523](#)
- [Monitoring and Troubleshooting the CC-Group Selection in Rulebase, on page 524](#)

Feature Description

This feature is introduced to customize the behavior for different types of subscribers in the Assume Positive scenario. This customization is made by enabling the users to specify a desired Credit-Control (CC) group based on the rulebase dynamically selected by PCRF.

Typically, the behavior for Assume Positive is configured within the CC group. In releases prior to 20, there were options to choose the CC group through APN/subscriber-profiles, IMSA, or AAA configurations. In this release, the CC group selection functionality is extended to rulebase configuration.

This feature is explicitly required in scenarios where IMSA was not used, AAA server could not send CC group during authentication, and only a single APN/subscriber-profile was used for all the subscribers. In such situations, this feature targets to provide a premium CC group within rulebase to enable premium treatment to subscribers based on their types.

This feature introduces a new configurable option inside the rulebase configuration, so that the users can specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This configured CC group overrides or has a higher priority than the CC group configured within the subscriber profile/APN. If the AAA or PCRF server sends the CC-Group AVP, the CC group value defined through the AVP overrides the rulebase configured CC group.

When this feature is enabled, the configuration allows specifying an association between the rulebase name and the CC group so that when a premium subscriber connects, a premium rulebase and a premium CC group are selected.

**Important**

Mid-session configuration change will not impact the existing subscribers in the system. This configuration change will be effected only to the new sessions.

Implementing this new configuration option enables different types of Assume-Positive behavior for subscribers based on the available quota. This results in achieving preferential treatment for premium customers.

The precedence order for selection of the CC group is defined as:

- PCRF provided CC group
- AAA provided CC group
- Rulebase configured CC group
- Subscriber Profile/APN selected CC group
- Default Credit-Control group

**Important**

This feature should not be used when there is an option for AAA server to send the CC group during authentication process. If during the authentication, AAA server sends a CC group, and the rulebase selected has a CC group defined within, then the rulebase defined CC group is selected for the session.

Limitations

There are no limitations or restrictions with this feature. However, it is important to keep in mind the precedence order for CC group selection.

Configuring Credit-Control Group in Rulebase

The following sections provide the configuration commands to configure the Credit-Control Group based on the rulebase of the subscriber.

Defining Credit-Control Group

The following commands are used to configure a desired Credit-Control group name when using the rulebase selected by PCRF.

```
configure
require active-charging
active-charging service service_name
rulebase rulebase_name
credit-control-group cc_group_name
end
```

- *cc_group_name*: Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

- **no credit-control-group:** Removes the previously configured CC group from the rulebase configuration. This is the default setting.
- This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.
- This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers.
- If this CLI command is configured, the selection of the CC group will be based on the precedence order. That is, the rulebase defined CC group has higher precedence over the CC group value specified in the Subscriber/APN profile.
- If the CC group configuration is not present in the rulebase, the default subscriber/APN profile configuration is applied.

Verifying the Credit-Control Group Configuration

Use the following command in Exec mode to display/verify the configuration of CC group in rulebase.

show configuration verbose

Monitoring and Troubleshooting the CC-Group Selection in Rulebase

This section provides information regarding show commands and/or their outputs in support of this feature.

show active-charging sessions full

The output of this show CLI command displays the selected credit-control-group for the session. The output details are useful in verifying and troubleshooting the issues with this feature.

show configuration errors

This show CLI will list an error if the credit-control group that is configured inside the rulebase is not defined.

show configuration verbose

This command will show the "credit-control-group" option specified for the rulebase. For troubleshooting purpose, capture the output of **show configuration verbose** and **show subscribers full** along with the **monitor-protocol** output containing "Radius Access-Accept".

Combined CCR-U Triggering for QoS Change Scenarios

In release 20, the number of CCR-Us sent to the OCS is controlled for QoS change scenarios in P-GW call. This new behavior is introduced in the system to easily handle the issues with Transactions Per Second (TPS) on OCS.

In releases prior to 20, for a change in the default EPS bearer QoS and APN AMBR received from PCRF for LTE or S2b WiFi calls, P-GW used to send two separate CCR-Us to OCS through Gy interface, one each for QoS change and AMBR change. In 20 and later releases, when default EPS bearer QoS and APN AMBR values are changed, P-GW sends update request to access side to change default bearer and APN AMBR in a single message. P-GW will apply APN AMBR and default bearer QoS accordingly and will send only one CCR-U on Gy for this change condition.

**Important**

This behavior change is applicable only to P-GW calls. This change has no impact to the Rf/CDR records, and GGSN/P-GW eHRPD calls.

Also, note that this behavior is not applicable for split TFT case (QoS + APN AMBR + TFT) wherein multiple Update Bearer Requests are sent towards the access side.

Re-activating Offline Gy Session after Failure

This section describes the feature to re-enable Offline Gy session on detecting failure at Diameter Credit Control Application.

This section includes the following topics:

Feature Description

With this feature, a mechanism to re-enable the Offline Gy session back to Online charging, based on indication from PCRF is introduced in this release. Upon receiving the Online AVP from PCRF, the gateway will establish the Gy session.

In previous releases, there was no provision to activate Gy once the session was marked as Offline. On detecting failure at Diameter Credit Control Application, the configured Credit Control Failure Handling (CCFH) action would be taken. Once the Gy session has taken the CCFH Continue action, the subscriber session could not be retried/re-enabled.

The Online AVP in the Charging-Rule-Definition is considered as the trigger/indication from PCRF to enable the Offline Gy session, after the CCFH Continue action been taken. The Online AVP at the command level from PCRF will not be considered as a trigger to enable the Offline Gy session. As per 3GPP 29.212 (release 12.12.0), the Online AVP (1009) is an optional AVP inside the Charging-Rule-Definition grouped AVP (1003).

Limitations and Restrictions

This section lists the limitations and configuration restrictions with this feature:

- This feature is limited only to Volume Quota mechanism. Special handling is not done for Quota-Validity-Time (QVT) and Quota-Hold-Time (QHT) timers. When the Gy session goes offline and comes back again, these timers are not started. The timers will be started only when the next CCA-U provides the information from OCS.
- When the Gy session is marked Online, CDR closure is not required and this is handled by the billing system.
- This feature is not extended to the event-based credit-control sessions.
- When the CCFH action is taken due to MSCC level failure, the existing behavior is retained and the following behavior is observed:
 - CCFH Continue – Continue the category (MSCC) without charging at Gy and this is applicable to the MSCC (not to the entire session). The MSCC state in the output of the **show active-charging sessions full** command will display "No Charge".
 - CCFH Terminate/Retry-and-Terminate – The bearer gets terminated.

- When the Result-Code 4011 (DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE) is received at MSCC level, the category is marked Free-of-Charge and no further accounting for this category is done. When this result code is received at command level, the Gy session is made Offline. The Offline Gy session can be made Online again using the Online AVP from PCRF and the accounting will resume normally (CCR-U will be seen at OCS for this session).
- When CCFH Continue is configured and CCR-I failure occurs, the following behavior is observed:
 - Diabase Error – When diabase error (TCP connection down) occurs, the Gy session is marked Offline and the session-state is maintained (session-ID created). When re-enabling the Gy session, a new CCR-I is sent immediately (without waiting for data).
 - Response Timeout – When the response timeout happens, if the CCR-I is sent at session-setup and the session-setup timeout happens before response-timeout, then the bearer itself will be terminated. The **diameter send-crri traffic-start** configuration can be used optionally so that the CCR-I timeout does not affect the bearer creation.
 - When the Gy session goes Offline due to CCR-I response timeout and the Gy session is marked Online, the same Session-ID will be used.
 - If the Gy session went offline due to CCR-I error response, the session-information is deleted (next session-ID used will be different).
- In case of rule-movement across bearers (LTE to WiFi or vice-versa) where the Online rule is moved/associated to an existing bearer, the status of the Gy session is not changed.
- The trigger for marking the Offline Gy Session to Online is only based on the Online AVP received from the PCRF in the Charging-Rule-Definition.

Configuring Offline Gy Session after Failure

The following section provides the configuration commands to re-enable the offline Gy session.

Re-enabling Offline Gy Session

Use the following configuration to re-enable offline Gy session after failure.

```
configure
  active-charging service service_name
    credit-control
      [ no ] offline-session re-enable
    end
```

Notes:

- When **offline-session re-enable** is configured and the PCRF installs/modifies a rule with "Online" AVP value set to 1, then the Offline DCCA will be marked Online.
- The default configuration is **no offline-session re-enable**. This feature is disabled by default and when disabled only the **show configuration verbose** command will display this configuration.

Verifying the Configuration

Use the following command to verify the offline/online state transition timestamp:

```
show active-charging sessions full
```

Monitoring and Troubleshooting the Offline Gy Session after Failure

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed to troubleshoot any failure related to this feature:

- The CLI output of the **show active-charging sessions full** command can be verified. The "Last State Change Time" field indicates the timestamps at which a session went Offline and came back Online.
- The messages from **monitor subscriber next-call** command can be enabled with "verbosity 3" to analyze the message exchanges happening for the subscriber.
- The "acsmgr" and "debug" level logs can be enabled for further debugging.

show active-charging sessions full

The following new fields are added to the output of this command to display the state transition timestamp:

- Last State Change Time:
 - Offline/Online – The Offline timestamp is updated when the Gy session goes Offline. The Online timestamp is updated when the session is back Online.

Suppress AVPs

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature.

Feature Description

This feature adds enhancement to the *Support MVNO Information in Gx, Gy and CDRs* feature. SAEGW sends MVNO-Reseller-ID and MVNO-Subclass-ID AVPs in the Gy messages towards the OCS and CDR, whenever these AVPs are received by SAEGW from the PCRF.

With this enhancement, this behavior is now CLI controlled and a new CLI command has been introduced to suppress the AVPs being sent in the Gy interface.

Old Behavior: Reseller-id and subclass-id AVPs were sent in Gy when the same were received from PCRF for the ATT dictionary.

New Behavior: New CLI command **suppress_avp** has been added which allows to suppress the Reseller-id and subclass-id AVPs.

Command Changes

suppress_avp

New CLI command has been added to the Credit Control Group configuration mode to suppress the AVPs. Configuring this CLI command would suppress the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

```
configure
  active-charging service <acs_service_name>
```

```

    credit-control group <group_name>
        diameter suppress-avp reseller-id subclass-id
        [ no | default ] diameter suppress-avp reseller-id subclass-id
    end

```

Notes:

- **no:** Disables AVP suppression. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.
- **default:** Sets the default configuration. AVPs are not suppressed by default. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.
- **suppress-avp:** Suppresses both MVNO-subclassid and MVNO-Reseller-id AVPs.
- **reseller-id:** Suppresses the MVNO-Reseller-Id AVP.
- **subclass-id:** Suppresses the MVNO-Sub-Class-Id AVP.

Performance Indicator Changes

show configuration

This command has been modified to display the following output:

```

credit-control group default
    diameter origin endpoint sundar
    diameter peer-select peer minid1 secondary-peer minid2
    diameter session failover
    diameter dictionary dcca-custom32
    failure-handling initial-request continue
    failure-handling update-request continue
    diameter dynamic-rules request-quota on-traffic-match
    diameter suppress-avp reseller-id subclass-id

```

Configuring Gy Interface Support

To configure Gy interface support:

-
- Step 1** Configure the core network service as described in this Administration Guide.
- Step 2** Configure Gy interface support as described in the sections [Configuring GGSN / P-GW / IPSG Gy Interface Support, on page 529](#) and [Configuring HA / PDSN Gy Interface Support, on page 530](#).
- Step 3** Configure Event-based Gy support as described in [Configuring PLMN and Time Zone Reporting, on page 531](#).
- Step 4** *Optional.* Configure OCS Unreachable Failure Handling Feature or Assume Positive for Gy Feature as described in [Configuring Server Unreachable Feature, on page 532](#).
- Step 5** *Optional.* Configure Static Rulebase for CCR as described in [Configuring Static Rulebase for CCR, on page 533](#).
- Step 6** *Optional.* Configure Gy for GTP based S2a/S2b as described in [Configuring Gy for GTP based S2a/S2b, on page 533](#).
- Step 7** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Important** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.
-

Configuring GGSN / P-GW / IPSG Gy Interface Support

To configure the standard Gy interface support for GGSN/P-GW/IPSG, use the following configuration:

```
configure
context <context_name>
    diameter endpoint <endpoint_name>
        origin realm <realm>
        origin host <diameter_host> address <ip_address>
        peer <peer> realm <realm> address <ip_address>
    exit
active-charging service <ecs_service_name>
    credit-control [ group <cc_group_name> ]
        diameter origin endpoint <endpoint_name>
        diameter peer-select peer <peer> realm <realm>
        diameter pending-timeout <timeout_period>
        diameter session failover
        diameter dictionary <dictionary>
        failure-handling initial-request continue
        failure-handling update-request continue
        failure-handling terminate-request continue
    exit
exit
context <context_name>
    apn <apn_name>
```

```

selection-mode sent-by-ms
ims-auth-service <service>
ip access-group <access_list_name> in
ip access-group <access_list_name> out
ip context-name <context_name>
active-charging rulebase <rulebase_name>
credit-control-group <cc_group_name>
end

```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring HA / PDSN Gy Interface Support

To configure HA / PDSN Gy interface support, use the following configuration:

```

configure
context <context_name>
    diameter endpoint <endpoint_name>
        origin realm <realm>
        origin host <diameter_host> address <ip_address>
        peer <peer> realm <realm> address <ip_address>
    exit
exit
active-charging service <ecs_service_name>
    ruledef <ruledef_name>
        ip any-match = TRUE
    exit
    charging-action <charging_action_name>
        content-id <content_id>
        cca charging credit rating-group <rating_group>
    exit
    rulebase <rulebase_name>
        action priority <action_priority> ruledef <ruledef_name> charging-action
        <charging_action_name>
    exit
    credit-control [ group <cc_group_name> ]
        diameter origin endpoint <endpoint_name>
        diameter peer-select peer <peer> realm <realm>
        diameter pending-timeout <timeout>
        diameter session failover
        diameter dictionary <dictionary>
        failure-handling initial-request continue
        failure-handling update-request continue

```

```

failure-handling terminate-request continue
pending-traffic-treatment noquota buffer
pending-traffic-treatment quota-exhausted buffer
exit
exit
context <context_name>
  subscriber default
    ip access-group <acl_name> in
    ip access-group <acl_name> out
    ip context-name <context_name>
    active-charging rulebase <rulebase_name>
    credit-control-group <cc_group_name>
  end

```

Notes:

- For information on configuring IP access lists, refer to the *Access Control Lists* chapter in the *System Administration Guide*.
- For more information on configuring ECS ruledefs, refer to the *ACS Ruledef Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS charging actions, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- For more information on configuring ECS rulebases, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring PLMN and Time Zone Reporting

PLMN and Time Zone Reporting feature requires a credit-control group to be defined in the APN or subscriber configuration or there must be a default credit-control group configured. The following CLI commands are available to enable/disable PLMN and Time Zone Reporting feature.

To enable PLMN and Time Zone Reporting through subscriber-template, use the following configuration:

```

configure
context <context_name>
  subscriber name <subscriber_name>
    dns primary <primary_ipaddress>
    dns secondary <secondary_ipaddress>
    ip access-group test in
    ip access-group test out
    ip context-name <context_name>
    credit-control-client event-based-charging
    active-charging rulebase <rulebase_name>
  exit
end

```

Notes:

- The **credit-control-client event-based-charging** command should be used to enable PLMN and Time Zone Reporting.

For more information on configuring PLMN and Time Zone Reporting feature, refer to the *Command Line Interface Reference*.

To enable PLMN and Time Zone Reporting through APN template, use the following configuration:

```
configure
context <context_name>
  apn <apn_name>
    selection-mode sent-by-ms
    accounting-mode none
    ip access-group test in
    ip access-group test out
    ip context-name <context_name>
    ip address pool name <pool_name>
    credit-control-client event-based-charging
    active-charging rulebase <rulebase_name>
  exit
end
```

Rest of the parameters needed for Event-based Gy such as dictionary, endpoint will be picked from the credit-control group.

In a scenario where the triggers are configured through the CLI command and another set of triggers are also received from Gx, then the triggers from Gx will have a higher priority.

Configuring Server Unreachable Feature

The Server Unreachable feature requires a failure handling behavior to be defined in the Diameter Credit Control configuration. The following CLI commands are available to enable/disable OCS Unreachable Failure Handling feature.

To enable OCS Unreachable Failure Handling feature, use the following configuration:

```
configure
require active-charging
  active-charging service <service_name>
    credit-control
      servers-unreachable { initial-request | update-request } { continue | terminate } [ {
after-interim-volume <bytes> | after-interim-time <seconds> } + server-retries <retry_count> ]
      servers-unreachable behavior-triggers { initial-request | update-request } transport-failure
[ response-timeout | tx-expiry ]
      servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code
[ to end-result-code ] } }
      servers-unreachable behavior-triggers update-request { result-code { any-error | result-code
[ to end-result-code ] } }
    end
```

Notes:

- This CLI command "servers-unreachable { initial-request | update-request } { continue | terminate } [{ after-interim-volume ..." allows configuring interim-volume and interim-time in the following ways:
 - after-interim-volume <bytes> alone followed by server-retries.
 - after-interim-time <secs> alone followed by server-retries.
 - after-interim-volume <bytes> after-interim-time <secs> followed by server-retries.

- This CLI command **"servers-unreachable behavior-triggers"** is used to trigger the servers-unreachable failure handling at either Tx expiry or Response timeout (This CLI is similar to retry-after-tx-expiry in **"failure-handling update-request continue retry-after-tx-expiry"** command.).
- This CLI command **"servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code | to end-result-code } }"** is used to trigger the servers-unreachable failure handling based on the configured Diameter error result codes.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Static Rulebase for CCR

To allow static configuration of rulebase name to be passed to OCS via CCR message, use the following configuration:

```
configure
require active-charging
active-charging service service_name
credit-control group ccgroup_name
charging-rulebase-name rulebase_name
no charging-rulebase-name
end
```

Notes:

- By default, the rulebase obtained from APN/subscriber template will be sent to OCS through the CCR message.

For more information on configuring this feature, refer to the *Command Line Interface Reference*.

Configuring Gy for GTP based S2a/S2b

To provide Gy Support for WiFi integration in P-GW for GTP based S2a/S2b, use the following configuration:

```
configure
require active-charging
active-charging service service_name
credit-control group ccgroup_name
diameter update-dictionary-avps 3gpp-rel11
[ default | no ] diameter update-dictionary-avps
end
```

Notes:

- **3gpp-rel11**: Provides support for 3GPP Rel.11 specific AVPs in the standard Gy dictionary.

Gathering Statistics

This section explains how to gather Gy related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for ECS sessions.	show active-charging sessions full
Detailed information for the Active Charging Service (ACS)	show active-charging service all
Information on all rule definitions configured in the service.	show active-charging ruledef all
Information on all charging actions configured in the service.	show active-charging charging-action all
Information on all rulebases configured in the service.	show active-charging rulebase all
Statistics of the Credit Control application, DCCA.	show active-charging credit-control statistics
States of the Credit Control application's sessions, DCCA.	show active-charging credit-control session-states [rulebase <rulebase_name>] [content-id <content_id>]



ICAP Interface Support

This chapter provides information on configuring the external Active Content Filtering servers for a core network service subscriber. This chapter also describes the configuration and commands that are used to implement this feature.

It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in respective product Administration Guide, before using the procedures in this chapter.

The following products currently support ICAP interface functionality:

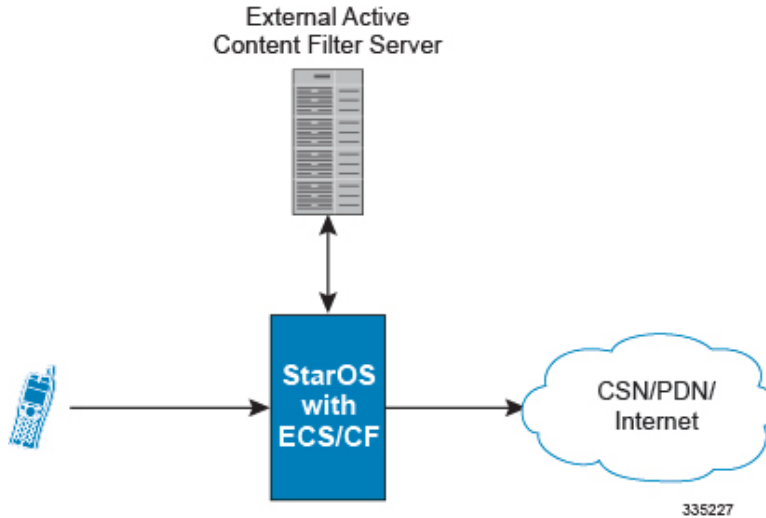
- GGSN
- P-GW
- [ICAP Interface Support Overview, page 535](#)
- [Configuring ICAP Interface Support, page 540](#)

ICAP Interface Support Overview

This feature supports streamlined ICAP interface to leverage Deep Packet Inspection (DPI) to enable external application servers to provide their services without performing DPI, and without being inserted in the data flow. For example with an external Active Content Filtering (ACF) Platform.

A high-level view of the streamlined ICAP interface support for external ACF is shown in the following figure:

Figure 69: High-Level View of Streamlined ICAP Interface with external ACF



The system with ECS is configured to support DPI and the system uses this capability for content charging as well. WAP and HTTP traffic is content filtered over the ICAP interface. RTSP traffic that contains adult content can also be content filtered on the ICAP interface. Only the RTSP Request packets will be considered for content filtering over the ICAP interface.

If a subscriber initiates a WAP (WAP1.x or WAP2.0) or Web session, the subsequent GET/POST request is detected by the DPI function. The URL of the GET/POST request is extracted and passed, along with subscriber identification information and the subscriber request, in an ICAP message to the application server. The application server checks the URL on the basis of its category and other classifications like, type, access level, content category and decides if the request should be authorized, blocked, or redirected by answering to the GET/POST with:

- A 200 OK message if the request is accepted.
- A 302 Redirect message in case of redirection. This redirect message includes the URL to which the subscriber must be redirected.
- Deny-response code 200 for RTSP requests is not supported. Only 403 "Forbidden" deny-response code will be supported.

Depending on the response received, the system with ECS will either pass the request unmodified, or discard the message and respond to the subscriber with the appropriate redirection or block message.

Content charging is performed by the Active Charging Service (ACS) only after the request has been controlled by the application server. This guarantees the appropriate interworking between the external application and content-based billing. In particular, this guarantees that charging will be applied to the appropriate request in case of redirection, and that potential charging-based redirections (i.e. Advice of Charge, Top Up page, etc.) will not interfere with the decisions taken by the application server.

Functions of the ACF include:

- Retrieval of subscriber policies based on the subscriber identity passed in the ICAP message

- Determining the appropriate action (permit, deny, redirect) to take for the type of content based on subscriber profile
- Communication of the action (permit, deny, or redirect) decision for the URL back to the ACS module

Supported Networks and Platforms

This feature supports the Cisco ASR 5500 platform for the core network services configured on the system.

For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

License Requirements

External Content Filtering Server support through Internet Content Adaptation Protocol (ICAP) interface is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Failure Action on Retransmitted Packets

ICAP rating is enabled for retransmitted packet when default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios. In these cases the retransmitted packet in the uplink direction is sent for ICAP rating again.

In case of WAP CO, uplink retransmitted packet for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request) then uplink retransmitted packet for each of the transaction is sent for rating again.

In case of HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken is sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP request for the same flow (pipelined request) then for the retransmitted packet the URL that will be sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on re-transmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
 - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.
 - Content Insert: The retransmitted packet is not sent for ICAP rating.
 - Redirect: The retransmitted packet is not sent for ICAP rating.

- Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
 - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.
- HTTP:
 - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even though the rating was redirect or content insert.
 - Content Insert: Retransmitted packets are dropped and not charged.
 - Redirect: Retransmitted packets are dropped and not charged.
 - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
 - Terminate flow: Retransmitted packets are dropped and not charged.
 - RTSP:

The following scenarios describe the failure actions where an RTSP request is received from the client. If ICAP is enabled, then the request goes to the ICAP server for content filtering.

- Allow: If the failure action configured is "allow", the RTSP request packet is sent out after applying the appropriate disposition action. Here, the flow remains the same as in the case if the ICAP response received is 200 OK.
- Content Insert: If the failure action configured is "content-insertion <string of size 1 to 128>", then this failure action for RTSP request will not be supported. Instead the failure action "Discard" for such an RTSP request will be supported.
- Redirect-URL: If the failure action configured is "redirect-url <string of size 1 to 128>", then a TCP FIN_ACK packet with an RTSP "302 Moved Temporarily" response header is inserted towards the client containing the said URL for redirection. A TCP RST packet is inserted towards the server. The underlying TCP connection is thus closed. If the RTSP client wants to retry to the redirected URL, the opening of a new TCP connection must be initiated.
- Discard: If the failure action configured is "discard", then the RTSP request packet received from the client is quietly discarded and no notification is sent to the client.
- Terminate flow: If the failure action configured is "terminate-flow", then the TCP connection is torn down by injecting a TCP FIN-ACK towards the client and a RST packet towards the server. However, no notification will be sent to the RTSP client and the server regarding this flow termination.

ICAP Client Communication with RFC 3507 compliance

The ICAP Content Filtering solution is extended to support ICAP client communication with ICAP server on Cisco ASR 5500 P-GW and HA in compliance with RFC 3507 - Internet Content Adaptation Protocol (ICAP).

Only HTTP Request modification and partial enhancement of error codes per RFC 3507 is addressed in this release. The ICAP client running on P-GW/HA communicates with external ICAP server over ICAP protocol. If content filtering is enabled for a subscriber, all HTTP GET requests from that subscriber are validated by the content filtering server (ICAP server), and is allowed, denied or redirected depending on the content categorization request.

Content-Filtering can be enabled for subscribers either through Override Control (OC) feature for predefined and static rules, or L7 Dynamic Rule Activation feature. A configurable option is added in the Content Filtering Server Group Configuration Mode to configure ICAP header that includes two parameters - Subscriber number information and CIPA (Children's Internet Protection Act) category.



Important

Override Control and L7 Dynamic Rule Activation are license-controlled features. A valid feature license must be installed prior to configuring these features. Contact your Cisco account representative for more information.

- **Subscriber Number:** The "Subscription ID" AVP is sent from gateway to PCRF in CCR message. The AVP values are received to the gateway from HSS. The gateway does not receive this AVP in CCI-A message.
- **CIPA category:** The category string will be provided by PCRF and is included as an extension header in ICAP request modification message. The AVP will be received from PCRF in CCA-I or RAR.

Dictionary and AVP Support

A new Content Filtering (CF) dictionary "custom4" is introduced and the following new AVPs are added to r8-gx-standard and custom4 dictionaries.

- **Override-Content-Filtering-State:** This attribute carries information about Content Filtering status (CF state) of rules or charging-action. This AVP is used for overriding the content-filtering status of static and predefined rules. This attribute is included in the Override-Control grouped AVP.
- **CIPA:** This attribute contains the Children's Internet Protection Act (CIPA) category string value that is treated as an ICAP plan identifier. This identifier helps ICAP server in locating the correct Content Filtering plan i.e. CIPA category based on which the packet is processed.

This attribute value is received from PCRF over Gx interface and is included in ICAP header while sending ICAP request.

- **L7-Content-Filtering-State:** This attribute carries information about Content Filtering status (CF state) of L7 rules. This attribute indicates whether or not the ICAP functionality is enabled or disabled for L7 charging rule definition received for installation from PCRF. Based on this attribute value, the traffic matching to the dynamic rule is sent to ICAP server.

This attribute is included in the L7-Application-Description grouped AVP for L7 rule processing. This is applicable only for HTTP protocol.



Important

CIPA and flags for controlling content filtering via OC and L7 Dynamic Rules features is applicable only for r8-gx-standard dictionary.

In addition to the new AVP support, L7-Field AVP in the L7-Application-Description grouped AVP is encoded to additionally accept ANY-MATCH as the input. The current framework does not support the existing field

"vlan-id" in Override-Control, which is present in charging action. Hence, the Override-Content-Filtering-State AVP replaces Override-VLAN-ID to support OC.

When subscriber initiates create session request, P-GW/HA sends CCR-I message to PCRF to obtain subscriber profile. PCRF responds with CCA-I message that contains CIPA and OC information if ICAP functionality is enabled for this subscriber.

In the case of L7 dynamic rules, the Content-Filtering capability is enabled by sending L7-Content-Filtering-State AVP in L7-Application-Description grouped AVP. At least one L7 filter should be present when L7-Content-Filtering-State is received for the dynamic rule. If L7-Content-Filtering-state AVP is sent along with L7 filter information AVP, then the Content-Filtering state will not be considered. Hence, the filter received with L7-Content-Filtering-State will not be processed and the L7 rule will be discarded.

In the case of Override Control, when content filtering is enabled for subscriber, PCRF sends ICAP flag through Override-Control AVP. This AVP overwrites charging action to enable ICAP feature for that subscriber.

Refer to the *AAA Interface Administration and Reference* for more information on the supported AVPs.

Limitations

The limitations for this feature are listed below:

- Only IPv4 addressing scheme is supported.
- ICAP content filtering is applicable only for HTTP traffic. HTTPS traffic is not supported by ICAP client.
- Accelerated path will not be supported for this feature.

Configuring ICAP Interface Support

This section describes how to configure the Content Filtering Server Group (CFSG) through Internet Content Adaptation Protocol (ICAP) interface between ICAP client and ACF server (ICAP server).



Important

This section provides the minimum instruction set for configuring external content filtering servers on ICAP interface on the system. For more information on commands that configure additional parameters and options, refer to *CFSG Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to provide ICAP interface support for external content filtering servers:

-
- Step 1** Create the Content Filtering Server Group and create ICAP interface with origin (local) IP address of chassis by applying the example configuration in [Creating ICAP Server Group and Address Binding, on page 541](#).
- Step 2** Specify the active content filtering server (ICAP server) IP addresses and configure other parameters for ICAP server group by applying the example configuration in [Configuring ICAP Server and Other Parameters, on page 541](#).
- Step 3** Configure the content filtering mode to external content filtering server group mode in ECS rule base by applying the example configuration in [Configuring ECS Rulebase for ICAP Server Group, on page 542](#).
- Step 4** Configure the charging action to forward HTTP/RTSP/WAP GET request to external content filtering servers on ICAP interface in Active Charging Configuration mode by applying the example configuration in [Configuring Charging Action for ICAP Server Group, on page 543](#).
- Step 5** Verify your ICAP interface and external content filtering server group configuration by following the steps in [Verifying the ICAP Server Group Configuration, on page 543](#).
- Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Creating ICAP Server Group and Address Binding

Use the following example to create the ICAP server group and bind the IP addresses:

```
configure
context <icap_ctxt_name> [ -noconfirm ]
content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]
    origin address <ip_address>
end
```

Notes:

- <ip_address> is local IP address of the CFSG endpoint.

Configuring ICAP Server and Other Parameters

Use the following example to configure the active content filtering (ICAP server) and other related parameters:

```
configure
context <icap_context_name>
content-filtering server-group <icap_server_grp_name>
    icap server <ip_address> [ port <port_number> ] [ max <max_msgs> ] [ priority <priority> ] [
standby ]
    connection retry-timeout <retry_timeout>
    deny-message <msg_string>
    dictionary { custom1 | custom2 | custom3 | custom4 | standard }
    failure-action { allow | content-insertion <content_string> | discard | redirect-url <url> |
terminate-flow }
    header extension options { cipa-category cipa_category_name | subscriber-number
subscriber_num_name } +
```

```
response-timeout <timeout>
end
```

Notes:

- In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In release 8.0, only one ICAP Server can be configured per Content Filtering Server Group.
- The **standby** keyword can be used to configure the ICAP server as standby. A maximum of ten active and standby ICAP servers per Content Filtering Server Group can be configured. The active and standby servers under the same server group can be configured to work in active-standby mode.
- The maximum outstanding request per ICAP connection configured using the optional **max** <max_msgs> keyword is limited to one. Therefore, any other value configured using the **max** keyword will be ignored.
- *Optional.* To configure the ICAP URL extraction behavior, in the Content Filtering Server Group configuration mode, enter the following command:

```
url-extraction { after-parsing | raw }
```

By default, percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters and sent.

- The **custom4** dictionary is a custom-defined dictionary that specifies user-defined information in the ICAP request message. The ICAP request message includes subscriber number and CIPA category values.

When **custom4** dictionary is configured, ICAP requests are formed as part of ICAP RFC 3507 request mode request. If any other dictionary is configured, the earlier implementation of ICAP client will not be partial RFC compliant.

- The **header extension options** command configures ICAP header parameters - subscriber number and CIPA category.

Configuring ECS Rulebase for ICAP Server Group

Use the following example to configure the content filtering mode to ICAP server mode in the ECS rulebase for content filtering:

```
configure
require active-charging [ optimized-mode ]
active-charging service <acs_svc_name> [ -noconfirm ]
rulebase <rulebase_name> [ -noconfirm ]
content-filtering mode server-group <cf_server_group>
end
```

Notes:

- In release 8.1, the **optimized-mode** keyword enables ACS in the Optimized mode, wherein ACS functionality is managed by SessMgrs. In release 8.1, ACS must be enabled in the Optimized mode.
- In release 8.3, the **optimized-mode** keyword is obsolete. With or without this keyword ACS is always enabled in Optimized mode.
- In release 8.0 and release 9.0 and later, the **optimized-mode** keyword is not available.

Configuring Charging Action for ICAP Server Group

Use the following example to configure the charging action to forward HTTP/WAP GET request to ICAP server for content processing.

```
configure
active-charging service <acs_svc_name>
charging-action <charging_action_name> [ -noconfirm ]
[ no ] content-filtering processing server-group
end
```

Notes:

- If the content-filtering flag supplied by charging action is required to configure the Override Control feature, then the **no content-filtering processing** command must be configured. This will ensure overriding content-filtering processing to be enabled or disabled through the Override Control feature.

Verifying the ICAP Server Group Configuration

This section explains how to display and review the configurations after saving them in a .cfg file and also to retrieve errors and warnings within an active configuration for a service.



Important

All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the configuration for this feature.

Step 1

Verify your ICAP Content Filtering Server Group configuration by entering the following command in Exec Mode:

show content-filtering server-group

The following is a sample output. In this example, an ICAP Content Filtering server group named *icap_cfsg1* was configured.

```
Content Filtering Group:      icap_cfsg1
Context:                    icap1
Origin Address:             1.2.3.4
ICAP Address(Port):         1.2.3.4(1344)
Max Outstanding:            256
Priority:                    1
Response Timeout: 30(secs)  Connection Retry Timeout: 30(secs)
Dictionary:                 standard
Timeout Action:             terminate-flow
Deny Message:              "Service Not Subscribed"
URL-extraction:             after-parsing
Header Extension Options:    subscriber-number i-sub
Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria: 1
```

Step 2

Verify any configuration error in your configuration by entering the following command in Exec Mode:

show configuration errors



IP Header Compression

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product administration guide, before using the procedures in this chapter.



Important

RoHC header compression is not applicable for SGSN and GGSN services.

- [Overview, page 545](#)
- [Configuring VJ Header Compression for PPP, page 546](#)
- [Configuring RoHC Header Compression for PPP, page 547](#)
- [Configuring Both RoHC and VJ Header Compression, page 549](#)
- [Configuring RoHC for Use with SO67 in PDSN or HSGW Service, page 550](#)
- [Using an RoHC Profile for Subscriber Sessions, page 552](#)
- [Disabling VJ Header Compression Over PPP, page 554](#)
- [Disabling RoHC Header Compression Over SO67, page 555](#)
- [Checking IP Header Compression Statistics, page 556](#)
- [RADIUS Attributes for IP Header Compression, page 557](#)

Overview

The system supports IP header compression on the PPP tunnels established over the EVDO-RevA A10 links and also over the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67).

By default IP header compression using the VJ algorithm is enabled for subscribers using PPP.

Note that you can use the default VJ header compression algorithm alone, configure the use of RoHC header compression only, or use both VJ and RoHC IP header compression.

- **Van Jacobsen (VJ)** - The RFC 1144 (CTCP) header compression standard was developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.
- **RObust Header Compression (RoHC)** - The RFC 3095 (RoHC) standard was developed in 2001. This standard can compress IP/UDP/RTP headers to just over one byte, even in the presence of severe channel impairments. This compression scheme can also compress IP/UDP and IP/ESP packet flows. RoHC is intended for use in wireless radio network equipment and mobile terminals to decrease header overhead, reduce packet loss, improve interactive response, and increase security over low-speed, noisy wireless links.

**Important**

The RoHC is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

In addition, you can configure RoHC profiles that define RoHC Compressor and Decompressor parameters. These RoHC profiles can be applied to subscribers.

You can also turn off all IP header compression for a subscriber.

The procedures in this chapter describe how to configure the IP header compression methods used, but for RoHC over PPP the Internet Protocol Control Protocol (IPCP) negotiations determine when they are used.

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead.
- Reduces packet loss rate over lossy links.

Configuring VJ Header Compression for PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

Note that procedure described in this section is applicable only when VJ header compression is disabled.

**Important**

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to enable VJ header compression to IP headers:

-
- Step 1** Enable VJ header compression by applying the example configuration in [Enabling VJ Header Compression, on page 547](#).
- Step 2** Verify your VJ header compression configuration by following the steps in [Verifying the VJ Header Compression Configuration, on page 555](#).
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Enabling VJ Header Compression

Use the following example to enable the VJ header compression over PPP:

```
configure
  context <ctxt_name>
    subscriber name <subs_name>
      ip header-compression vj
    end
```

Notes:

- <ctxt_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <subs_name> is the name of the subscriber in the current context that you want to enable VJ IP header compression for.

Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show subscriber configuration username subs_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring RoHC Header Compression for PPP

RoHC IP header compression can be configured for all IP traffic, uplink traffic only, or downlink traffic only. When RoHC is configured for all traffic, you can specify the mode in which RoHC is applied.

**Important**

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to enable RoHC header compression to IP headers:

- Enable RoHC header compression by applying the example configuration in [Enabling RoHC Header Compression for PPP](#), on page 548.
- Verify your RoHC header compression configuration by following the steps in [Verifying the Header Compression Configuration](#), on page 548.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling RoHC Header Compression for PPP

Use the following example to enable the RoHC over PPP:

```
configure
  context <ctxt_name>
    subscriber name <subs_name>
      ip header-compression RoHC [ any [ mode { optimistic | reliable | unidirectional }
    ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr <value> | mrru <value> ] } |
    marked flows-only | max-hdr <value> | mrru <value> | downlink | uplink ] }+
  end
```

Notes:

- *<ctxt_name>* is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- *<subs_name>* is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

show subscriber configuration username *subs_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring Both RoHC and VJ Header Compression

You can configure the system to use both VJ and RoHC IP header compression. When both VJ and RoHC are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.



Important

If both RoHC and VJ header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.



Important

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to enable both RoHC and VJ header compression to IP headers:

- Enable the RoHC and VJ header compression by applying the example configuration in [Enabling RoHC and VJ Header Compression for PPP](#), on page 549.
- Verify your RoHC and VJ header compression configuration by following the steps in [Verifying the Header Compression Configuration](#), on page 550.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Enabling RoHC and VJ Header Compression for PPP

Use the following example to enable the header compression over PPP:

configure

context <ctxt_name>

subscriber name <subs_name>

ip header-compression vj RoHC [any [mode { optimistic | reliable | unidirectional }] | cid-mode { { large | small } [marked-flows-only | max-cid | max-hdr <value> | mrru <value> }] | marked flows-only | max-hdr <value> | mrru <value> | downlink | uplink }]+
end

Notes:

- <ctxt_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <subs_name> is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- Refer to the Subscriber Configuration Mode Commands chapter in Command Line Interface Reference for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

show subscriber configuration username *subs_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Configuring RoHC for Use with SO67 in PDSN or HSGW Service

This section explains how to set RoHC settings in the PDSN or HSGW Service configuration mode. These settings are transferred to the PCF during the initial A11 setup and are used for the GRE tunnel that is connected to the PCF to support EVDO-RevA Service Option 67 (SO67). RoHC is enabled through an auxiliary SO67 A10 connection and the PCF signals this information when the auxiliary A10 is connected.



Important

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *PDSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to enable the RoHC header compression feature at the PDSN or HSGW Service over SO67:

-
- Step 1** Enable header compression by applying the example configuration in [Enabling RoHC Header Compression with PDSN, on page 550](#) or [Enabling ROHC Header Compression with HSGW section, on page 551](#).
 - Step 2** Verify your RoHC configuration by following the steps in [Verifying the Header Compression Configuration, on page 551](#).
 - Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Enabling RoHC Header Compression with PDSN

Use the following example to enable the RoHC header compression with PDSN over SO67:

```
configure
  context <ctxt_name>
    pdsn-service <svc_name>
```

```

ip header-compression rohc
cid-mode {large | small} max-cid integer
mrru <num_octets>
profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }
end

```

Notes:

- <ctxt_name> is the system context in which PDSN service is configured and you wish to configure the service profile.
- <svc_name> is the name of the PDSN service in which you want to enable RoHC over SO67.
- Refer to the *PDSN Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Enabling RoHC Header Compression with HSGW

Use the following example to enable the RoHC header compression with HSGW over SO67:

```

configure
  context <ctxt_name>
    hsgw-service <svc_name>
      ip header-compression rohc
        cid-mode {large | small} max-cid integer
        mrru <num_octets>
        profile { [esp-ip] [rtp-udp] [udp-ip] [uncompressed-ip] }
      end
    end
end

```

Notes:

- <ctxt_name> is the system context in which HSGW service is configured and you wish to configure the service profile.
- <svc_name> is the name of the HSGW service in which you want to enable RoHC over SO67.
- Refer to the *HSGW Service RoHC Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context ctxt_name
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Using an RoHC Profile for Subscriber Sessions

You can configure RoHC profiles that specify numerous compressor and decompressor settings. These profiles can in turn be applied to a specific subscriber or the default subscriber. RoHC profiles are used for both RoHC over PPP and for RoHC over SO67.



Important

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to apply RoHC profile to a subscriber session:

-
- Step 1** Create RoHC profile using decompression mode or decompression mode. If you want to use compression mode go to step a else follow step b:
- Configure RoHC profile by applying the example configuration in the [Creating RoHC Profile for Subscriber using Compression Mode, on page 552](#) using compression mode.
 - Alternatively configure RoHC profile by applying the example configuration in the [Creating RoHC Profile for Subscriber using Decompression Mode, on page 553](#) using compression mode.
- Step 2** Apply existing RoHC profile to a subscriber by applying the example configuration in the [Applying RoHC Profile to a Subscriber, on page 553](#).
- Step 3** Verify your RoHC header compression configuration by following the steps in the [Verifying the Header Compression Configuration, on page 554](#).
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Creating RoHC Profile for Subscriber using Compression Mode

Use the following example to create RoHC profile for a subscriber using compression mode:

```
configure
  RoHC-profile profile-name <RoHC_comp_profile_name>
    decompression-options
      [no] multiple-ts-stride
      rtp-sn-p <p_value>
      [no] use-ipid-override
      [no] use-optimized-talkspurt
      [no] use-optimized-transience
      [no] use-timer-based-compression
    end
```

Notes:

- <RoHC_comp_profile_name> is the name of the RoHC profile with compression mode which you want to apply to a subscriber.

- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Compression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

Creating RoHC Profile for Subscriber using Decompression Mode

Use the following example to create RoHC profile for a subscriber using decompression mode:

```
configure
  RoHC-profile profile-name <RoHC_decomp_profile_name>
    decompression-options
      context-timeout <dur>
      max-jitter-cd <dur_ms>
      nak-limit <limit>
      optimistic-mode-ack
      optimistic-mode-ack-limit <num_pkts>
      piggyback-wait-time <dur_ms>
      preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable |
    unidirectional }
      rtp-sn-p <p_value>
      [no] rtp-sn-p-override
      [no] use-clock-option
      [no] use-crc-option
      [no] use-feedback
      [no] use-jitter-option
      [no] use-reject-option
      [no] use-sn-option
    end
```

Notes:

- <RoHC_profile_name> is the name of the RoHC profile with decompression mode which you want to apply to a subscriber.
- System configured most of the parameters by default. For more information on other options and parameters and details, refer to the *RoHC Profile Decompression Configuration Mode Commands* chapter in *Command Line Interface Reference*.

Applying RoHC Profile to a Subscriber

Once an RoHC profile has been created that profile can be specified to be used for a specific subscribers. Use the following example to apply the RoHC profile to a subscriber:

```
configure
  context <ctxt_name>
    subscriber name <subs_name>
      RoHC-profile-name <RoHC_profile_name>
    end
```

Notes:

- <ctxt_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.

- `<subs_name>` is the name of the subscriber in the current context that you want to enable RoHC header compression for.
- `<RoHC_profile_name>` is the name of the existing RoHC profile (created with compressed or decompressed mode) which you want to apply to a subscriber in the current context.
- Refer to the *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference* for more details on this command and its options.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

show subscriber configuration username *subs_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Disabling VJ Header Compression Over PPP

By default, VJ IP header compression is enabled for subscriber sessions. When VJ header compression is configured all IP headers are compressed using the VJ compression algorithm.

If you do not want to apply compression to any IP headers for a subscriber session you can disable the IP header compression feature.



Important

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *Subscriber Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable VJ header compression to IP headers:

- Step 1** Disable header compression by applying the example configuration in [Disabling VJ Header Compression](#), on page 555.
- Step 2** Verify your VJ header compression configuration by following the steps in [Verifying the VJ Header Compression Configuration](#), on page 555.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Disabling VJ Header Compression

Use the following example to disable the VJ header compression over PPP:

```
configure
  context <ctxt_name>
    subscriber name <subs_name>
      no ip header-compression
  end
```

Notes:

- <ctxt_name> is the system context in which you wish to configure the subscriber profile. Typically this is an AAA context.
- <subs_name> is the name of the subscriber in the current context that you want to disable IP header compression for.

Verifying the VJ Header Compression Configuration

These instructions are used to verify the VJ header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

show subscriber configuration username <subs_name>

The output of this command is a concise listing of subscriber parameter settings as configured.

Disabling RoHC Header Compression Over S067

If you do not want to apply compression to any IP headers for a subscriber sessions using the EVDO-RevA S067 feature, you can disable the IP header compression feature at the PDSN or HSGW Service.



Important

This section provides the minimum instruction set for configuring subscriber profile for header compression. For more information on commands that configure additional parameters and options, refer *PDSN Service Configuration Mode Commands* or *HSGW Service Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to disable the IP header compression feature at the PDSN or HSGW Service:

-
- Step 1** Disable header compression by applying the example configuration in [Disabling RoHC Header Compression](#), on page 556.
- Step 2** Verify your RoHC configuration by following the steps in [Verifying the Header Compression Configuration](#), on page 556.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Disabling RoHC Header Compression

Use the following example to disable the header compression over SO67:

```
configure
  context <ctxt_name>
    pdsn/hsgw-service <svc_name>
      no ip header-compression RoHC
    end
```

Notes:

- <ctxt_name> is the system context in which PDSN or HSGW service is configured and you wish to configure the service profile.
- <svc_name> is the name of the PDSN or HSGW service in which you want to disable RoHC over SO67.

Verifying the Header Compression Configuration

These instructions are used to verify the header compression configuration.

Verify that your header compression configurations for subscriber by entering the following command in Exec Mode in specific context:

```
show configuration context <ctxt_name>
```

The output of this command is a concise listing of subscriber parameter settings as configured.

Checking IP Header Compression Statistics

This section commands to use to retrieve statistics that include IP header compression information.

The following Exec mode commands can be used to retrieve IP header compression statistics:

- monitor protocol ppp

- show ppp
- show ppp statistics
- show RoHC statistics
- show RoHC statistics pdsn-service
- show subscriber full username

For more information on these commands, refer to the *Command Line Interface Reference*.

RADIUS Attributes for IP Header Compression

This section lists the names of the RADIUS attributes to use for RoHC header compression. For more information on these attributes, refer to the AAA Interface Administration and Reference.

One of the following attributes can be used to specify the name of the RoHC profile to use for the subscriber session:

- SN-RoHC-Profile-Name
- SN1-RoHC-Profile-Name

Any RoHC parameters not specified in the RoHC profile are set to their default values.



IP Pool Sharing Protocol

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

This chapter contains the following topics:

- [Overview, page 559](#)
- [How IPSP Works, page 561](#)
- [Configuring IPSP Before the Software Upgrade, page 564](#)
- [Configuring IPSP After the Software Upgrade, page 566](#)
- [Disabling IPSP, page 567](#)

Overview

The IP Pool Sharing Protocol (IPSP) is a protocol that system-based HA services can use during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity.

In order for IPSP to be used, at least two system-based HAs with identical configurations must be present on the same LAN. IPSP uses a primary & secondary model to manage the IP pools between the HAs. When used, this protocol ensures the following:

- In-progress sessions can be handed-off to the secondary HA when an offline-software upgrade is being performed on the primary and receive the same IP address that it was originally assigned.
- New sessions can be redirected to the secondary HA when an offline-software upgrade is being performed on the primary and receive a non-duplicate IP address.

The protocol is enabled at the interface level. Each system-based HA must have an IPSP-enabled interface configured in the same context as the HA service for this protocol to function properly.

Primary HA Functionality

The primary HA is the system that is to be upgraded. It performs the following functions for IPSP:

- Queries the pool information from the secondary HA the pool configurations on both HAs must be identical
- Assigns an IP address or address block to the secondary HA when requested by the secondary HA the primary HA releases sessions if they have an IP address requested by the secondary
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), sends a termination message to the secondary HA causing it to assume the responsibilities of the primary HA until the primary is available again.
- Sends a trap when the number of calls drops to zero after starting IPSP

Secondary HA Functionality

The secondary HA is the system that takes over Mobile IP sessions from the primary HA that is being upgraded. It performs the following functions for IPSP:

- Locks the IP pools until it receives an address or address block assignment from the primary HA it unlocks the IP pools after busying out the addresses that are not assigned to it
- Processes address requests for sessions that are within the address block assigned to it
- Communicates with the primary HA, as needed, to request IP addresses that are not currently assigned to it it does not assign the address until the primary HA approves it
- For graceful termination conditions (e.g. an administrative user issues the **reload** command), it notifies the primary HA that it is going out of service
- Assumes the responsibility of the primary HA when requested to
- In the event that it determines that primary HA is not available, it assumes the responsibility of the primary HA if there is at least one address allocated to verify that the AAA server is re-configured to direct the calls

Requirements, Limitations, & Behavior

- One IPSP interface can be configured per system context.
- The IPSP interfaces for both the primary and secondary HAs must be configured to communicate on the same network.
- If IP pool busyout is enabled on any configured address pool, IPSP can not be configured.
- The IP pool configuration (pool name, addresses, priority, pool group, etc.) on both the HAs must be identical.
- IP pools cannot be modified on either the primary or the secondary HAs once IPSP is enabled.
- Sessions are dropped during the IPSP setup process if:

- the primary HA has not yet approved an IP address or address block.
- the primary HA is not known to the secondary HA.
- Once an address is assigned to the secondary HA, all the information about that address is erased on the primary HA and that address becomes unusable by the primary HA.
- LRU is not supported across the systems. Although, LRU continues to be supported within the system.
- If the IPSP configuration is not disabled before removing the HA from the IPSP network link, sessions may be rejected if the system's VPN Manager is rebooted or restarts.
- IPSP does not control static IP pools. An external application (AAA, etc.) must be responsible for ensuring that duplicate addresses are not assigned.
- IPSP ignores interface failures allowing the configured dead-interval timer to determine when the HA should become the primary and control the pool addresses. Before the dead-interval timer starts, the secondary HA maintains its state and any busied out addresses remain busied out. After the dead-interval timer starts, IPSP marks the neighboring peer HA as down, becomes primary, and will unbusy out all pool addresses.

How IPSP Works

IPSP operation requires special configuration in both the primary and secondary HAs. As mentioned previously, both HAs must have identical configurations. This allows the secondary HA to process sessions identically to the primary when the primary is taken offline for upgrade.

Configuration must also be performed on the AAA server. Whereas subscriber profiles on the AAA server originally directed sessions to the primary HA, prior to using IPSP, subscriber profiles must be re-configured to direct sessions to the secondary HA.

There are two scenarios in which IPSP takes effect:

- **New sessions:** Once IPSP is configured, new sessions are directed to a secondary HA (HA2) allowing the primary HA to go through a software upgrade without degrading network capacity. The secondary HA requests addresses from the primary HA's (HA1) pools as needed. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.
- **Session handoffs:** Once IPSP is configured, sessions originally registered with the primary HA (HA1) are re-registered with the secondary HA (HA2). To ensure the session is assigned the same IP address, the secondary HA requests the address from the primary HA. The primary HA verifies the binding and releases it to the secondary HA which, in turn, re-assigns it to the session. As the addresses are allocated, they are busied out on the primary HA. This procedure is displayed below.

IPSP Operation for New Sessions

The following figure and text describe how new sessions are handled when IPSP is enabled.

Figure 70: IPSP Operation for New Sessions

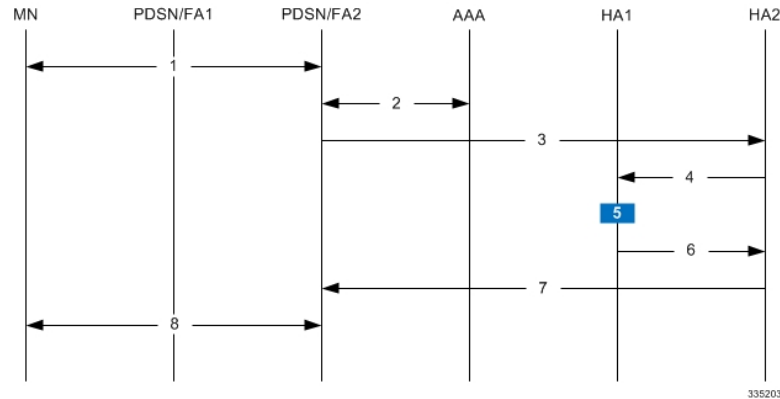


Table 37: IPSP Operation for New Sessions Description

Step	Description
1	A mobile node (MN) attempting to establish a data session is connected to PDSN/FA 2.
2	PDSN/FA 2 authenticates the subscriber with the AAA server. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
3	PDSN/FA 2 forwards the session request to HA2 for processing. HA2 processes the session as it would for any Mobile IP session.
4	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
5	HA1 allocates the address to HA2 and busies it out so it can not be re-assigned.
6	HA1 responds to HA2 with the IP address for the session.
7	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the MN.
8	The MN and PDSN/FA 2 complete session processing.

IPSP Operation for Session Handoffs

The following figure and text describe how session handoffs are handled when IPSP is enabled.

Figure 71: IPSP Operation for Session Handoffs

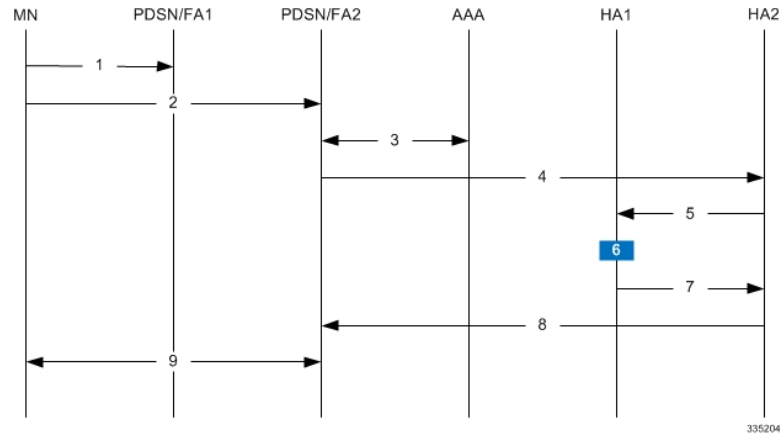


Table 38: IPSP Operation for Session Handoffs Description

Step	Description
1	A mobile node (MN) is connected to PDSN/FA 1.
2	The MN's session is handed-off to PDSN/FA2 and goes through the re-registration process.
3	PDSN/FA 2 authenticates the subscriber with the AAA server as part of the re-registration process. One of the attributes returned by the AAA server as part of a successful authentication is the IP address of the secondary HA.
4	PDSN/FA 2 forwards the session request to HA2 for processing. Included in the request is the MN's current IP address.
5	With IPSP enabled, prior to assigning an IP address, HA2 sends a request to HA1 for an IP address.
6	HA1 verifies the MN's information and releases the binding. It then busies out the address so it can not be re-assigned.
7	HA1 allocates the original IP address to HA2 for the session.
8	HA2 proceeds with session processing and provides PDSN/FA 2 with the IP address for the mobile node.
9	The mobile node and PDSN/FA 2 complete session processing.

Configuring IPSP Before the Software Upgrade

Configuring IPSP requires changes to the primary HA (the HA on which the software upgrade is to occur), the secondary HA (the HA to which subscribers sessions are to be directed), and the AAA server.

This section provides information and instructions for configuring IPSP before the software upgrade.



Important

This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To enable the IP pool sharing during software upgrade:

-
- Step 1** Configure the AAA servers by applying the example configuration in [Configuring the AAA Server for IPSP](#), on page 564.
 - Step 2** Configure an interface on the system for use by IPSP according to the instructions found in the *Creating and Configuring Ethernet Interfaces and Ports* section of the *System Administration Guide*.
 - Step 3** Enable the IPSP on secondary HA by applying the example configuration in [Enabling IPSP on the Secondary HA](#), on page 565.
 - Step 4** Perform the boot system priority and SPC/SMC card synchronization as described in *Off-line Software Upgrade* section in the *System Administration Guide*.
 - Step 5** Enable the IPSP on primary HA by applying the example configuration in [Enabling IPSP on the Primary HA](#), on page 565.
 - Step 6** Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration* section.
 - Step 7** Proceed for software upgrade as described in *Off-line Software Upgrade* section in the *System Administration Guide*.
 - Step 8** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Configuring the AAA Server for IPSP

For subscriber session establishment, the AAA server provides the IP address of the HA that is to service the session. This information exists in the 3GPP2_MIP_HA_Address RADIUS attribute configured for the subscriber.

Because the primary HA has been responsible for facilitating subscriber sessions, its IP address is the one configured via this attribute. For IPSP however, the attribute configuration must change in order to direct sessions to the secondary HA.

To do this, reconfigure the 3GPP2_MIP_HA_Address RADIUS attribute for each subscriber on the AAA server with the IP address of the secondary HA.

The precise instructions for performing this operation vary depending on the AAA server vendor. Refer to the documentation for your AAA server for more information.

Enabling IPSP on the Secondary HA

The secondary HA is the alternate HA that is to take responsibility while the primary HA is upgraded.



Important

This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on secondary HA:

```
configure
context <ipsp_ctxt_name> [ -noconfirm ]
interface <ipsp_if_name>
pool-share-protocol primary <pri_ha_address> [ mode {active | inactive | check-config } ]
dead-interval <dur_sec>
end
```

Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the primary HA's IPSP interface.
- *ipsp_if_name* is the name of the interface on which you want to enable IPSP.
- *dead-interval* is an optional command to configure time to wait before retrying the primary HA for the IP Pool Sharing Protocol.

Enabling IPSP on the Primary HA

The primary HA is the HA that is to be upgraded.



Important

This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on primary HA:

```
configure
context <ipsp_ctxt_name> [ -noconfirm ]
interface <ipsp_if_name>
pool-share-protocol secondary <sec_ha_address> [ mode {active | inactive | check-config } ]
dead-interval <dur_sec>
end
```

Notes:

- The interface must be configured in the same context as the HA service and must be on the same network as the secondary HA's IPSP interface.
- *ipsp_if_name* is the name of the interface on which you want to enable IPSP.
- *dead-interval* is an optional command to configure time to wait before retrying the secondary HA for the IP Pool Sharing Protocol.

**Important**

Once this configuration is done, the primary HA begins to hand responsibility for sessions and release IP addresses to the secondary HA. Prior to performing the software upgrade, all IP addresses must be released. When IPSP has released all IP pool addresses from the primary HA an SNMP trap (**starIPSPAllAddrsFree**) is triggered.

Verifying the IPSP Configuration

These instructions are used to verify the IPSP configuration.

Verify that IPSP has released all IP addresses by entering the following command in Exec Mode with in specific context:

show ip ipsp

The output of this command provides the list of used addresses and released addresses. The system will send the **starIPSPAllAddrsFree** trap once all IP addresses are released. When the value in the *Used Addresses* column reaches 0 for all IP pools listed, then the primary HA sends the SNMP trap and notifies the secondary HA to take over as the primary HA.

Configuring IPSP After the Software Upgrade

If desired, IP pool addresses can be migrated from the original secondary HA back to the original primary HA once the upgrade process is complete.

**Important**

It is important to note that the HA that was originally designated as the secondary is now functioning as the primary HA. Conversely, the HA that was originally designated as the primary is now functioning as the secondary.

In order to migrate the addresses, both HAs and the AAA server must be configured according to the instructions in this section.

This section provides information and instructions for configuring IPSP after the software upgrade.

**Important**

This section provides the minimum instruction set for configuring IPSP on the system. For more information on commands that configure additional parameters and options, refer *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To enable the IP pool sharing after software upgrade:

-
- Step 1** Configure the AAA servers by applying the example configuration in [Configuring the AAA Server for IPSP](#), on page 564.
 - Step 2** Configure an interface on the system for use by IPSP according to the instructions found in the Creating and Configuring Ethernet Interfaces and Ports section of *System Administration Guide*.
 - Step 3** Enable the IPSP on secondary HA by applying the example configuration in [Enabling IPSP on the Secondary HA](#), on page 565.
 - Step 4** Enable the IPSP on primary HA by applying the example configuration in [Enabling IPSP on the Primary HA](#), on page 565.
 - Step 5** Verify your ACL configuration by following the steps in the *Verifying the IPSP Configuration*.
 - Step 6** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Disabling IPSP

Once all IP addresses on the primary HA have been released, IPSP must be disabled on both the primary and secondary HAs.



Caution

Prior to disabling IPSP, ensure that the primary HA has released all IP addresses to secondary HA.

Follow the instructions in this section to disable IPSP on primary and secondary HA after migration of all IP addresses.



Important

This section provides the minimum instruction set for disabling IPSP on the HAs. For more information on commands, refer to the *IPSP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Use the following example to enable the IPSP on primary/secondary HA:

```
configure
context <ipsp_ctxt_name> [ -noconfirm ]
interface <ipsp_if_name>
no pool-share-protocol
end
```

Notes:

- The interface must be configured in the same context as the primary/secondary HA service and must be on the same network as the primary/secondary HA's IPSP interface.
- *ipsp_if_name* is the name of the interface on which you want to disable IPSP.
- IPSP must be disabled on both the HAs.



IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

This chapter describes the IPv6 Delegation feature.

- [Feature Description, page 569](#)

Feature Description

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into the following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
- IPv6 Interface ID from the RADIUS Server

IPv6 Prefix Delegation from the RADIUS Server



Important

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the delegated prefix from the RADIUS server to the UE or the CPE.

To enable the prefix delegation from the RADIUS server, first configure the APN on the P-GW. See [Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 572](#)

How It Works

This section describes functionality of the prefix delegation from the RADIUS server.

During initial authentication process, RADIUS AAA can authorize Framed-IPv6-Address and Delegated-IPv6-Prefix AVP. Prior to the introduction of this feature Cisco P-GW was able to process only Framed-IPv6-Address AVP. This AVP was treated as Default-Prefix for the attaching UE. P-GW used to allocate 64-bit Interface-ID and the combined 128-bit address. The 64-bit default-prefix, derived from Framed-IPv6-Address AVP, and locally generated 64-bit Interface-ID was sent to the UE during this initial attachment. This 64-bit default-prefix was then associated with the default bearer/PDN for the UE and is considered as the UE's IPv6 address.

With the introduction of this feature, P-GW is able to process Delegated-IPv6-Prefix AVP along with Framed-IPv6-Address. Delegated-IPv6-Prefix AVP is used to designate the Delegated Prefix of prefix length 48/52/56 bits. This AVP is treated differently than Framed-IPv6-Address. P-GW communicates this delegated prefix to the UE only using DHCPv6 message handshake SOLICIT/ADVERTISE/REQUEST/RESPONSE. Delegated-IPv6-Prefix is not associated with the default bearer and it is not considered as the UE IPv6 address.

- 1 Configure the APN on the P-GW, to enable the prefix delegation from the RADIUS server. For the configuration steps, see [Configuring APN to Enable Prefix Delegation From RADIUS Server, on page 572](#).
- 2 Configure APN on the P-GW for the prefix delegation. RADIUS server may send delegated prefix in the Access-Accept message independent of the APN configuration on the P-GW. Based on the APN configuration and presence of delegate prefix in the Access-Accept message, the following combinations are possible. The PDN setup is rejected if:
 - The RADIUS server has not sent Delegated Prefix in the Access-Accept message
 - The **pd-alloc-method** in the APN configuration is **no-dynamic**

The following table lists all possible combination of the APN configuration and presence of delegated prefix in the Access-Accept message:

Table 39: Mapping of APN Configuration and RADIUS Message

pd-alloc-method in APN Configuration	Delegated-IPv6-Prefix in Access-Accept RADIUS Message	PDN State
no-dynamic	Yes	PDN is set up if: <ul style="list-style-type: none"> • The delegated prefix is successfully allocated after level1 and level2 validations are done • Validation with the static pool, as mentioned in step 3, is successful If validation fails, PDN is not set up.
no-dynamic	No	PDN is not set up.

pd-alloc-method in APN Configuration	Delegated-IPv6-Prefix in Access-Accept RADIUS Message	PDN State
local/dhcpv6-proxy	Yes	Delegated-IPv6-Prefix in Access-Accept RADIUS message is discarded. PDN is set up. Delegate prefix is allocated to the UE, on receiving SOLICIT message, based on the configured pd-alloc-method in the APN.
local/dhcpv6-proxy	No	PDN is set up. Delegated prefix is allocated to the UE, on receiving SOLICIT message, based on the configured pd-alloc-method in the APN.

- 3 The P-GW then performs the following two level validation for the prefix length received in Access-Accept RADIUS message:

Level 1: Prefix length must be only one of the supported values, such as, 48 / 52 / 56. For any other length, delegate prefix is rejected and PDN is not set up.

Level 2: If level 1 validation is passed, the prefix length is compared with the **prefix-delegation-len** configured in the APN using the CLI command, **ipv6 address prefix-delegation-len**.

If there is a mismatch, delegate prefix is rejected and PDN is not set up.



Important

Level2 validation is not done if prefix-delegation-len is not configured in the APN.

- 4 Only if the above two level validation is successful, the received delegate prefix is validated against the **static** ipv6 prefix pool configured in the destination context. If validation with the static pool is successful, then the delegate prefix is stored on the P-GW. If validation with the static pool fails, the delegate prefix is rejected and PDN is not set up.
- 5 After the PDN is set up, the UE or the CPE sends a delegated prefix request by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix, which it had stored earlier, in the DHCPv6 ADVERTISE message to the UE.
- 6 Next, the UE sends the DHCPv6 REQUEST message to the P-GW and the P-GW sends the DHCPv6 REPLY message to the UE, which completes the DHCPv6 handshake.
- 1 When the DHCPv6 RELEASE message is received from the UE, P-GW blocks data from any sources IP address from the delegated prefix pool. The delegated prefix is not released to the static ipv6 prefix pool from which it was allocated. If the DHCPv6 SOLICIT message is received again from the UE, the same delegate prefix is sent to the UE. The P-GW starts passing the data from the source address part of the said delegated prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests delegated prefix release by sending DHCPv6 RELEASE REQUEST message to the P-GW.

The DHCPv6 RELEASE REPLY message is not sent to the UE and no message is sent to the RADIUS server if:

- The delegated prefix is released when validity time configured in the DHCPv6 service expires
- When the PDN is cleared

Release triggered reason can be checked from the DHCPv6 statistics(output of the CLI command **show dhcpv6 statistics**, which are as follows:

```
Session Release Reasons:(dhcp-prefix-delegation)
PDNs Released: 3          Lease Exp Policy: 0
UE Initiated Release: 1    Other Reasons: 0
```

- 7 When the PDN is cleared, the delegate prefix is released to the static ipv6 prefix pool from which it was allocated.

Configuring APN to Enable Prefix Delegation From RADIUS Server

Use the following syntax to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the RADIUS Server.

```
config
context context_name
  apn apn_name
    ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic ] allow-prefix-delegation
pd-alloc-method no-dynamic
  ipv6 address prefix-delegation-len [48 | 52 | 56]
end
```

Notes:

- **dhcpv6-proxy:** Configures the IPv6 address from DHCP server for the APN.
- **dhcpv6-proxy:** Configures the IPv6 address from DHCP server for the APN.
- **local:** Configures the IPv6 address from the local pool configured.
- **no-dynamic:** Configures the IPv6 address as indicated by the authentication server.
- **allow-prefix-delegation:** Configures the APN to allow DHCPv6 prefix-delegation.
- **ipv6 address prefix-delegation-len:** Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Verifying Prefix Delegation from the RADIUS Server

To verify the Prefix Delegation from the RADIUS Server, use the following show commands.

show dhcpv6 statistics

When APN is configured to receive Delegated Prefix from Radius Server, the sessions statistics is visible under CLI command output of **show dhcpv6 statistics** and displays the following output:

```
DHCPv6 Session Stats:
Total Current: 0
```



```

DHCP Proxy:          0
DHCP Server:         0
DHCP PD:             0
Radius PD:           0
Local PD:            0
Total Setup:         5
DHCP Proxy:          0
DHCP Server:         0
DHCP PD:             0
Radius PD:           1
Local PD:            4

Total Released:      5
DHCP Proxy:          0
DHCP Server:         0
DHCP PD:             0
Radius PD:           1
Local PD:            4

```

Notes:

- The total current counter is incremented while sending request reply message to the UE.
- The total current counter is decremented while sending release reply message to the UE (in case of UE initiated release) in the following two cases:
 - on valid life timer expiry
 - when PDN is cleared
- The total current counter may be incremented/decremented multiple times during a PDN connection.
- The total setup counter is incremented multiple times during the PDN connection lifetime. For example, every-time when the SOLICIT message is processed, the PD is successfully allocated to the UE.
- The total release counter is incremented multiple times during a PDN connection lifetime. For example, everytime when the PD is released when DHCPv6 RELEASE message is processed from the UE and/or PD is released due to VALID lifetime timer expiry event. Along with this Session Release Reasons: (dhcp-prefix-delegation) counters are also incremented to the corresponding release reasons.
-
- Hence in case of delegate prefix allocation from the RADIUS server, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all

This command displays the following output:

```

IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA

```

show sub pgw-only full all

This command displays the following output:

```

IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1

```

```
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

show sub saegw-only full all

This command displays the following output:

```
IPv6 allocation type: AAA
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56 Sent to UE: No
IPv6 prefix delegation alloc type: AAA
```

IPv6 Prefix Delegation from the Local Pool



Important

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

This feature allows the User Equipment (UE) or a Customer Premises Equipment (CPE) to request the delegated prefix, configured in the destination context, from the P-GW. P-GW then sends the prefix delegation from the local pool to the UE or the CPE.

To enable the prefix delegation from the local pool, first configure the APN on the P-GW. See [Configuring APN for Private Pool Name, on page 575](#) and [Configuring Prefix Delegation on Destination Context, on page 576](#)

How It Works

This section describes the functionality of the prefix delegation from the local pool.

- 1 Configure APN on the GGSN/P-GW/SAE-GW to enable the prefix delegation from the local pool. For configuration steps, see [Configuring APN for Private Pool Name, on page 575](#)
- 2 Once the APN is configured, configure the pool on destination context. See [Configuring Prefix Delegation on Destination Context, on page 576](#).
- 3 The PDN is first set up with default ipv6 prefix of length 64.
- 4 Once the PDN is set up, User Equipment (UE) or a Customer Premises Equipment (CPE) can request delegated prefix by sending DHCPv6 SOLICIT message to P-GW.
- 5 The P-GW then performs the following two level validation for the prefix length:

Level 1: The prefix length requested in DHCPv6 SOLICIT message must be only one of the supported values, 48 / 52 / 56. For any other length, the SOLICIT is silently dropped at P-GW.

Level 2: If level 1 validation is successful, then the following validation is done. If **prefix-delegation-len** is configured in the APN, then delegate prefix allocation of this length is attempted from the local private pool. If **prefix-delegation-len** is not configured in the APN, then delegate prefix allocation of length requested in SOLICIT message is attempted from the local private pool.

**Important**

The requested length for the delegate prefix must match with the prefix-length configured for the private pool. The requested prefix length is as configured in the APN as ipv6 address prefix-delegation-len 52. If it is not configured in the APN, it may also be from the SOLICIT message. Configure the prefix length for the private pool by using the CLI command, **ipv6 pool ipv6-private prefix 5001::1/48 prefix-length 52 private 0**. Only when these lengths match, delegated prefix allocation from the local pool is successful.

- 6 The UE or a CPE can request the delegated prefix by sending DHCPv6 SOLICIT message to the P-GW. P-GW sends the delegated prefix allocated from the local pool, in the DHCPv6 ADVERTISE message to the UE.
- 7 Next, the UE sends the DHCPv6 REQUEST message to the P-GW. The P-GW sends the DHCPv6 REPLY message to the UE, which completed the DHCPv6 handshake.

If the delegated prefix allocation from the local pool fails, the DHCPv6 SOLICIT message is silently dropped at the P-GW.

- 8 When the UE sends the DHCPv6 RELEASE message, the delegated prefix is released to the ipv6 prefix pool.

DHCPv6 RELEASE REPLY message is sent to the UE, only when the UE requests prefix delegation released by sending DHCPv6 RELEASE REQUEST message to the P-GW.

DHCPv6 RELEASE REPLY message is not sent to UE if:

- The prefix delegation is released when validity time configured in the DHCPv6 service expires
- The PDN is cleared

If DHCPv6 SOLICIT message is received again from the UE, a new delegated prefix is allocated from the local pool and sent to the UE.

Configuring APN to Enable Prefix Delegation From Local Pool

Configuration Overview

To enable prefix delegation from a local pool, perform the following steps:

- Step 1** Configure the private pool name in the APN configuration mode, to be used for delegate prefix allocation.
- Step 2** Configure the APN to enable or disable IPv6 prefix delegation or default prefix delegation from the local pool.

Configuring APN for Private Pool Name

Use the following steps to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the local pool:

config

```

context context_name
  apn apn_name
    ipv6 address delegate-prefix-pool pool_name
  no ipv6 address delegate-prefix-pool
end

config
  context context_name
    apn apn_name
      ipv6 address alloc-method [dhcpv6-proxy | local | no-dynamic ] allow-prefix-delegation
  pd-alloc-method local
    ipv6 address delegate-prefix-pool pool_name
    ipv6 address prefix-delegation-len [48 | 52 | 56]
  end

```

Notes:

- **delegate-prefix-pool:** Configures a pool of IPv6 address delegated prefix.
pool_name: Name of the pool with IPv6 address delegated prefix.
- **no:** Disables the pool of IPv6 address delegated prefix.
- **dhcpv6-proxy:** Configures the IPv6 address from the DHCP server for the APN.
- **local:** Configures the IPv6 address from the local pool configured.
- **allow-prefix-delegation:** Configures the APN to allow DHCPv6 prefix-delegation.
- **ipv6 address prefix-delegation-len:** Configures the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Configuring Prefix Delegation on Destination Context

Use the following configuration to configure the APN profile on the GGSN/P-GW/SAEGW for enabling Prefix Delegation from the Local Pool:

```

config
  context context_name
    ipv6 pool ipv6-private prefix 5001::1/48 prefix-length [48 | 52 | 56] private 0
  end

```

Notes:

- **ipv6 pool:** Modifies the current context's IP address pools by adding, updating, or deleting a pool. This command also resizes an existing IP pool.



Important

The ipv6 prefix pool must be of the type **private**.

Verifying Prefix Delegation from the Local Pool

To verify the Prefix Delegation from the local pool, use the following show commands.

show dhcpv6 statistics

When APN is configured to receive Delegated Prefix from the local pool, the sessions statistics is visible under CLI command output of **show dhcpv6 statistics** and displays the following output:

```
DHCPv6 Session Stats:
  Total Current:          0
  DHCP Proxy:            0
  DHCP Server:           0
  DHCP PD:               0
  Radius PD:             0
  Local PD:              0
Total Setup:             5
  DHCP Proxy:            0
  DHCP Server:           0
  DHCP PD:               0
  Radius PD:             1
  Local PD:              4

Total Released:          5
  DHCP Proxy:            0
  DHCP Server:           0
  DHCP PD:               0
  Radius PD:             1
  Local PD:              4
```

Notes: In case of delegate prefix allocation from local pool, Total Setup is equal to Total Current + Total Released.

show sub ggsn-only full all

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```

show sub pgw-only full all

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```

show sub saegw-only full all

The output of this command has been modified to display the following:

```
IPv6 allocation type: local
IP address: 4001::1122:aa33:bb44:cc55, 10.0.0.1
IPv6 delegated prefix : dddd:0:0:b000::/56
IPv6 prefix delegation alloc type: local
```

IPv6 Interface ID from the RADIUS Server

This feature allows the RADIUS/AAA Server to send an Interface-ID to the GGSN/P-GW/SAEGW service, in the Access-Accept message. This interface-id is used by these services and is communicated to the UE or the CPE. In this case, the GGSN/P-GW/SAEGW do not allocate a local interface-id. If the RADIUS/AAA server do not send an interface-id, then GGSN/P-GW/SAEGW allocate an interface-id locally and send it to the UE.

show apn statistics

Following CLI command can be used to see the total current active counter for Interface-ID allocation.

```
IP address allocation statistics:
Total IPv6 Interface IDs allocated:
  AAA provided:      1
  Locally Generated: 2
```

Limitations

Following are the limitations of the IPv6 Prefix Delegation feature:

- RADIUS ACCOUNTING messages do not support delegated prefix.
- Zero PL in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- NULL PD prefix in SOLICIT is not supported and the message is dropped silently. This is applicable for all methods of allocation of delegated prefix, including dhcpv6-proxy, local pool, and AAA.
- For PDN type v4v6, the dhcpv6-proxy method of allocation for the default prefix is not supported.
- The UE-requested Delegated Prefix in SOLICIT message is not supported. If the UE sends SOLICIT message requesting Delegated Prefix, it is rejected.
- One PD prefix per PDN is supported; multiple PD-prefixes per PDN are not supported.
- P-GW and GGSN do not support local-based and RADIUS-based allocation of both DHCPv6 prefix delegation and framed prefix delegation from the same pool. Hence the allocation is done from separate pools. Framed prefix received in the access-accept message is not part of the delegated prefix range.



L2TP Access Concentrator

This chapter describes the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) functionality support on Cisco® ASR 5500 chassis and explains how it is configured.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

The L2TP Access Concentrator is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

When enabled through the session license and feature use key, the system supports L2TP for encapsulation of data packets between it and one or more L2TP Network Server (LNS) nodes. In the system, this optional packet encapsulation, or tunneling, is performed by configuring L2TP Access Concentrator (LAC) services within contexts.



Important

The LAC service uses UDP ports 13660 through 13668 as the source port for sending packets to the LNS.

This chapter contains the following topics:

- [Applicable Products and Relevant Sections](#), page 580
- [Supported LAC Service Configurations for PDSN Simple IP](#), page 581
- [Supported LAC Service Configurations for the GGSN and P-GW](#), page 586
- [Supported LAC Service Configuration for Mobile IP](#), page 592
- [Configuring Subscriber Profiles for L2TP Support](#), page 595
- [Configuring LAC Services](#), page 599
- [Modifying PDSN Services for L2TP Support](#), page 601
- [Modifying APN Templates to Support L2TP](#), page 603

Applicable Products and Relevant Sections

The LAC feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Applicable Product(s)	Refer to Sections
PDSN/FA/HA	<ul style="list-style-type: none"> • <i>Supported LAC Service Configurations for PDSN Simple IP</i> • <i>Supported LAC Service Configuration for Mobile IP</i> • <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> • <i>RADIUS and Subscriber Profile Attributes Used</i> • <i>Configuring Local Subscriber Profiles for L2TP Support</i> • <i>Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</i> • <i>Configuring LAC Services</i> • <i>Modifying PDSN Services for L2TP Support</i>
GGSN/SGSN/FA/P-GW	<ul style="list-style-type: none"> • <i>Supported LAC Service Configurations for the GGSN</i> • <i>Supported LAC Service Configuration for Mobile IP</i> • <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> • <i>RADIUS and Subscriber Profile Attributes Used</i> • <i>Configuring Local Subscriber Profiles for L2TP Support</i> • <i>Configuring LAC Services</i> • <i>Modifying APN Templates to Support L2TP</i>
ASN GW	<ul style="list-style-type: none"> • <i>Supported LAC Service Configuration for Mobile IP</i> • <i>Configuring Subscriber Profiles for L2TP Support</i> <ul style="list-style-type: none"> • <i>RADIUS and Subscriber Profile Attributes Used</i> • <i>Configuring Local Subscriber Profiles for L2TP Support</i> • <i>Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes</i> • <i>Configuring LAC Services</i>

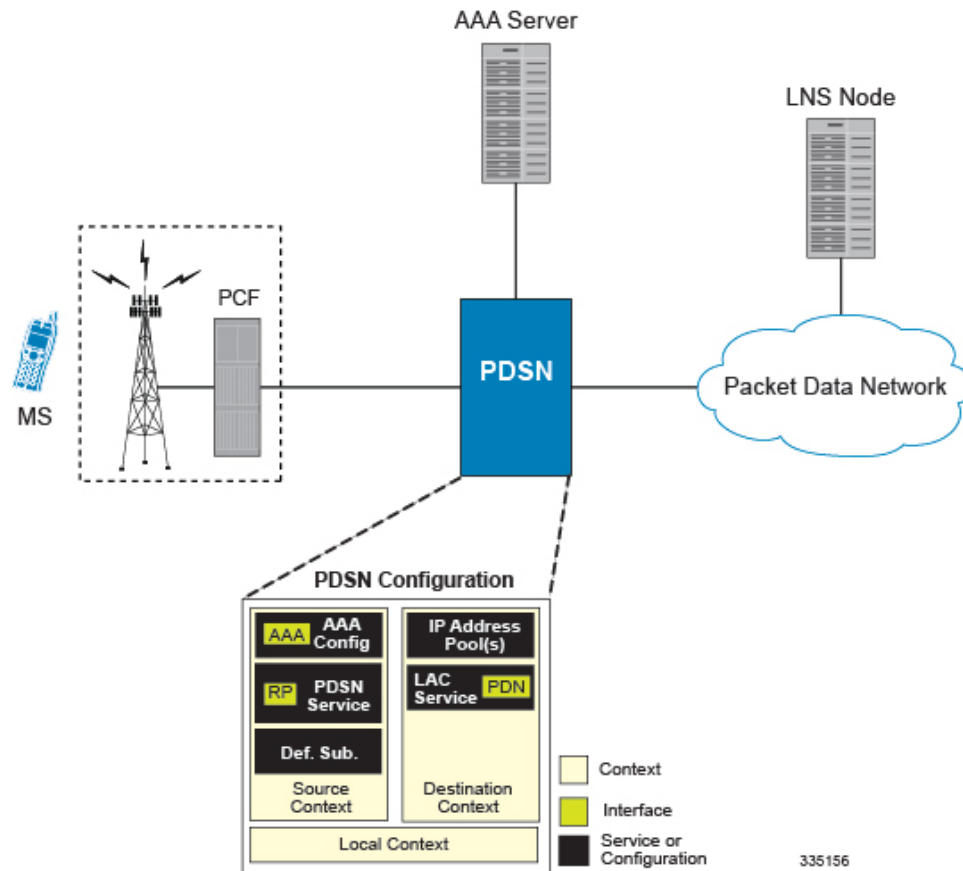
Supported LAC Service Configurations for PDSN Simple IP

LAC services can be applied to incoming PPP sessions using one of the following methods:

- **Attribute-based tunneling:** This method is used to encapsulate PPP packets for only specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.
- **PDSN Service-based compulsory tunneling:** This method of tunneling is used to encapsulate all incoming PPP traffic from the R-P interface coming into a PDSN service, and tunnel it to an LNS peer for authentication. It should be noted that this method does not consider subscriber configurations, since all authentication is performed by the peer LNS.

Each LAC service is bound to a single system interface configured within the same system context. It is recommended that this context be a destination context as displayed in the following figure.

Figure 72: LAC Service Configuration for SIP



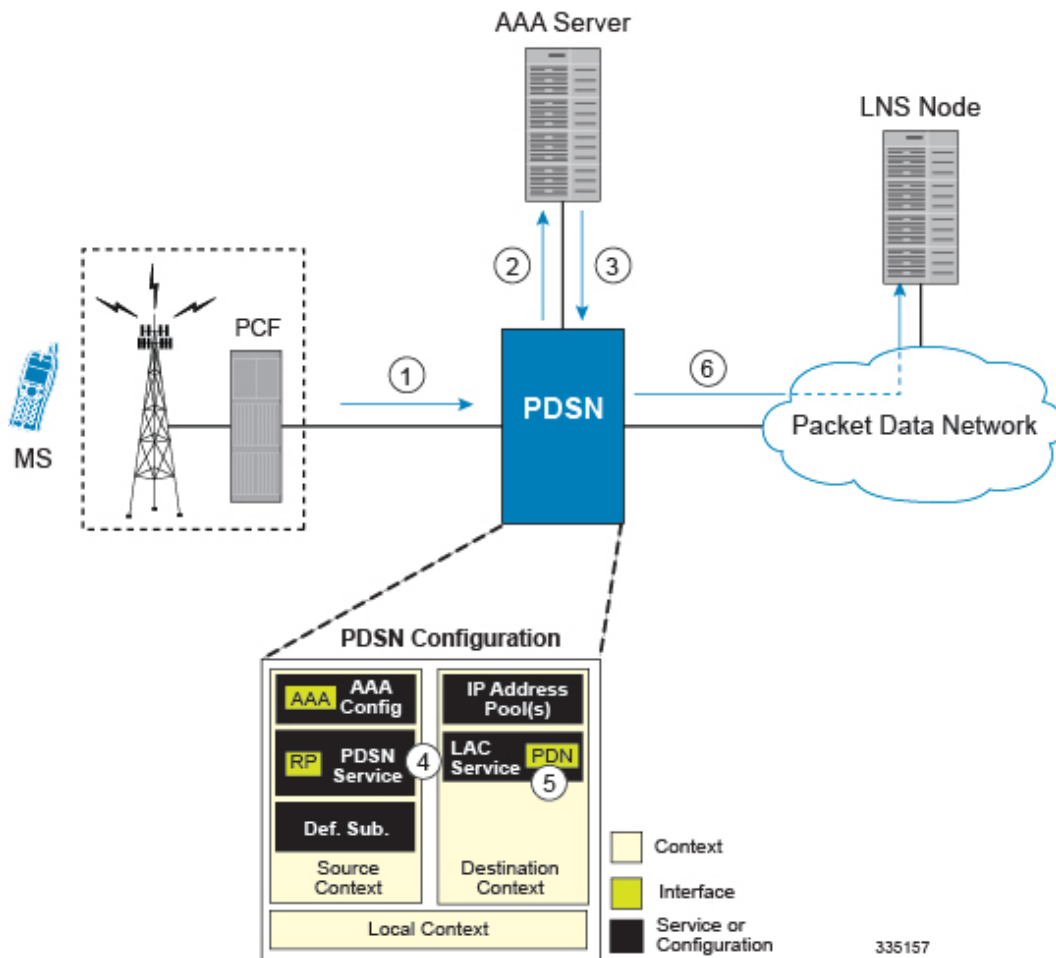
Attribute-based Tunneling

This section describes the working of attribute-based tunneling and its configuration.

How The Attribute-based L2TP Configuration Works

The following figure and the text that follows describe how Attribute-based tunneling is performed using the system.

Figure 73: Attribute-based L2TP Session Processing for SIP



- 1 A subscriber session from the PCF is received by the PDSN service over the R-P interface.
- 2 The PDSN service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
- 3 The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

- 4 The PDSN service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
- 5 The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
- 6 The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for PDSN Simple IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



Important

These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

-
- | | |
|---------------|---|
| Step 1 | Configure the subscriber profiles according to the information and instructions located in the <i>Configuring Subscriber Profiles for L2TP Support</i> section of this chapter. |
| Step 2 | Configure one or more LAC services according to the information and instructions located in the <i>Configuring LAC Services</i> section of this chapter. |
| Step 3 | Configure the PDSN service(s) with the tunnel context location according to the instructions located in the <i>Modifying PDSN Services for L2TP Support</i> section of this chapter. |
| Step 4 | Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration . For additional information on how to verify and save configuration files, refer to the <i>System Administration Guide</i> and the <i>Command Line Interface Reference</i> . |
-

PDSN Service-based Compulsory Tunneling

This section describes the working of service-based compulsory tunneling and its configuration.

How PDSN Service-based Compulsory Tunneling Works

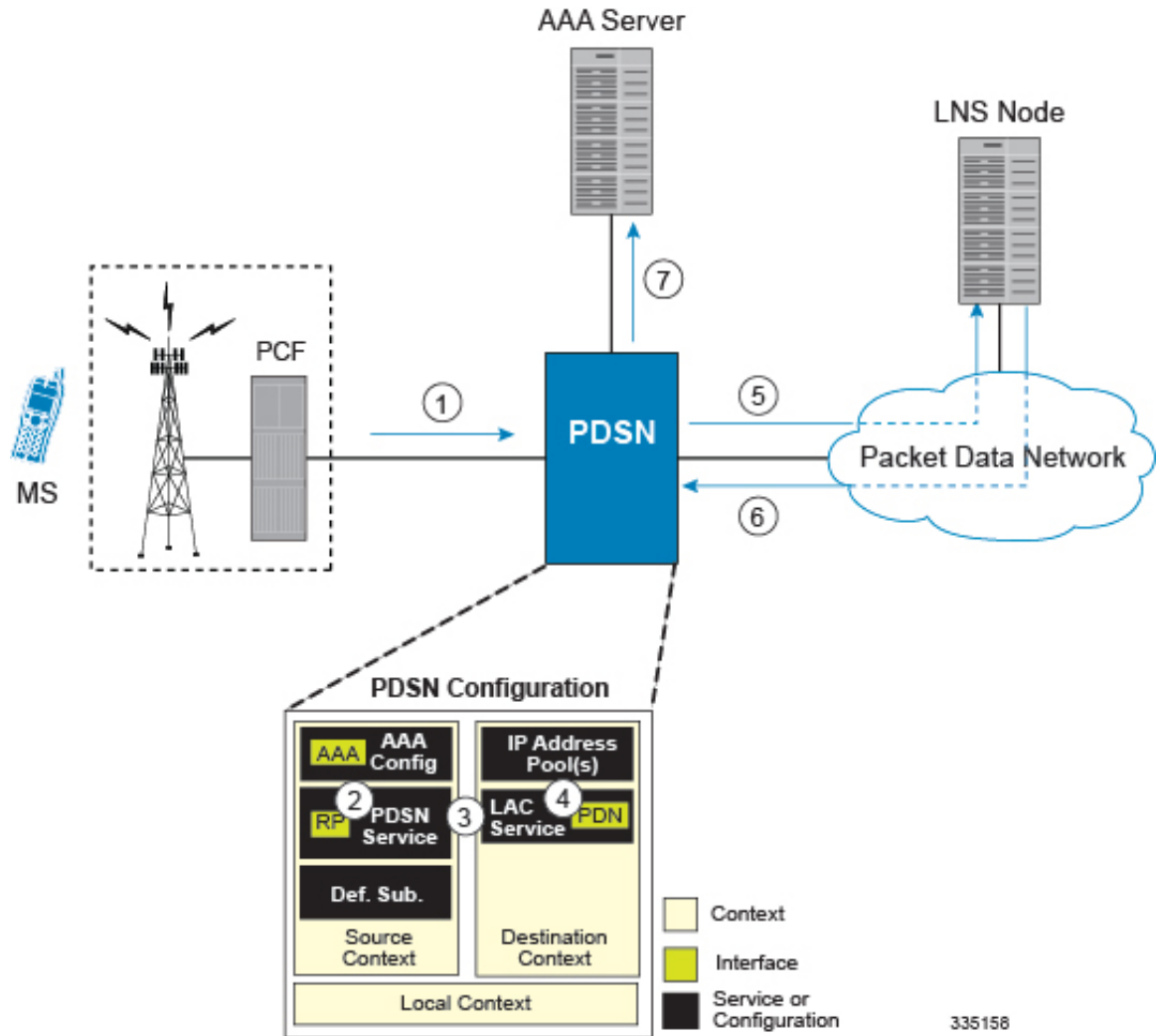
PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

Accounting start and interim accounting records are still sent to the local RADIUS server configured in the system's AAA Service configuration. When the L2TP session setup is complete, the system starts its call counters and signals the RADIUS server to begin accounting. The subscriber name for accounting records is based on the NAI-constructed name created for each session.

PDSN service-based compulsory tunneling requires the modification of one or more PDSN services and the configuration of one or more LAC services.

The following figure and the text that follows describe how PDSN service-based compulsory tunneling is performed using the system.

Figure 74: PDSN Service-based Compulsory Tunneling Session Processing



- 1 A subscriber session from the PCF is received by the PDSN service over the R-P interface.
- 2 The PDSN service detects its **tunnel-type** parameter is configured to L2TP and its **tunnel-context** parameter is configured to the Destination context.
- 3 The PDSN forwards all packets for the session to a LAC service configured in the Destination context. If multiple LAC services are configured, session traffic will be routed to each using a round-robin algorithm.
- 4 The LAC service initiates an L2TP tunnel to one of the LNS peers listed as part of its configuration.
- 5 Session packets are passed to the LNS over a packet data network for authentication.
- 6 The LNS authenticates the session and returns an Access-Accept to the PDSN.
- 7 The PDSN service initiates accounting for the session using a constructed NAI.

Session data traffic is passed over the L2TP tunnel established in step 4.

Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP

This section provides a list of the steps required to configure L2TP compulsory tunneling support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



Important

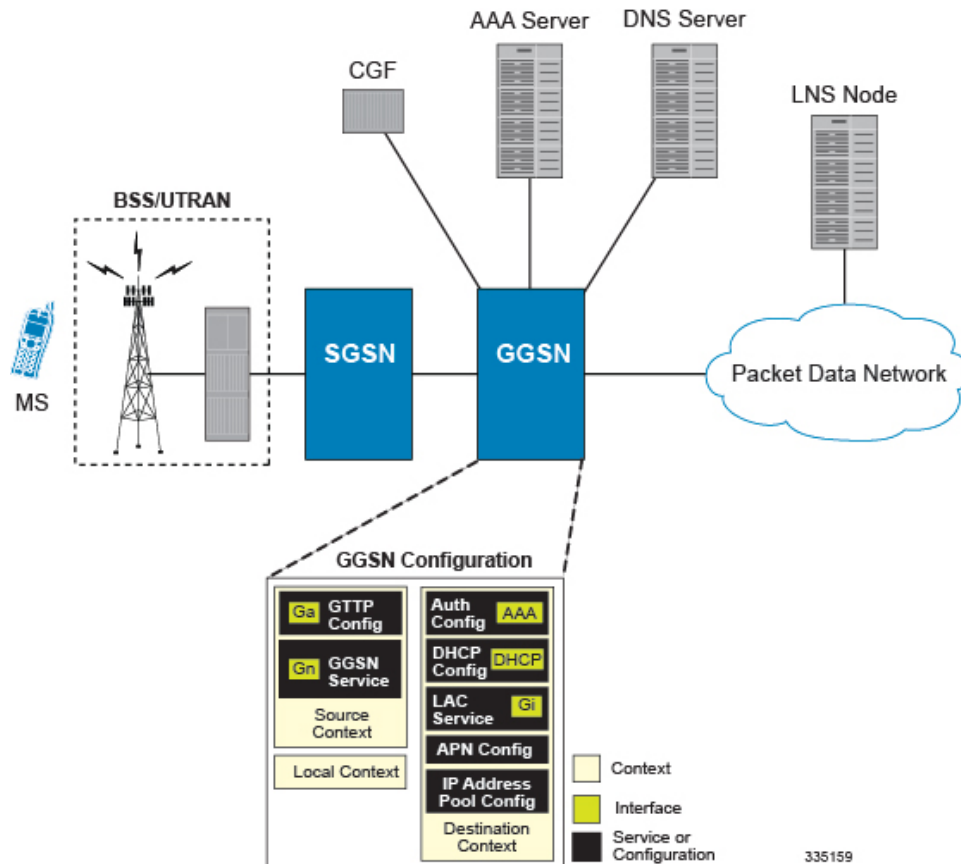
These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

-
- | | |
|---------------|---|
| Step 1 | Configure one or more LAC services according to the information and instructions located in the <i>Configuring LAC Services</i> section of this chapter. |
| Step 2 | Configure the PDSN service(s) according to the instructions located in the <i>Modifying PDSN Services for L2TP Support</i> section of this chapter. |
| Step 3 | Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration . For additional information on how to verify and save configuration files, refer to the <i>System Administration Guide</i> and the <i>Command Line Interface Reference</i> . |
-

Supported LAC Service Configurations for the GGSN and P-GW

As mentioned previously, L2TP is supported through the configuration of LAC services on the system. Each LAC service is bound to a single system interface configured within the same system destination context as displayed in following figure.

Figure 75: GGSN LAC Service Configuration



LAC services are applied to incoming subscriber PDP contexts based on the configuration of attributes either in the GGSN's Access Point Name (APN) templates or in the subscriber's profile. Subscriber profiles can be configured locally on the system or remotely on a RADIUS server.

LAC service also supports domain-based L2TP tunneling with LNS. This method is used to create multiple tunnels between LAC and LNS on the basis of values received in "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute received from AAA Server in Access-Accept as a key for tunnel selection and creation. When the LAC needs to establish a new L2TP session, it first checks if there is any existing L2TP tunnel with the peer LNS based on the value of key "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

If LAC service needs to establish a new tunnel for new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message. If all available peer-LNS are exhausted, LAC service will reject the call.

L2TP tunnel parameters are configured within the APN template and are applied to all subscribers accessing the APN. However, L2TP operation will differ depending on the subscriber's PDP context type as described below:

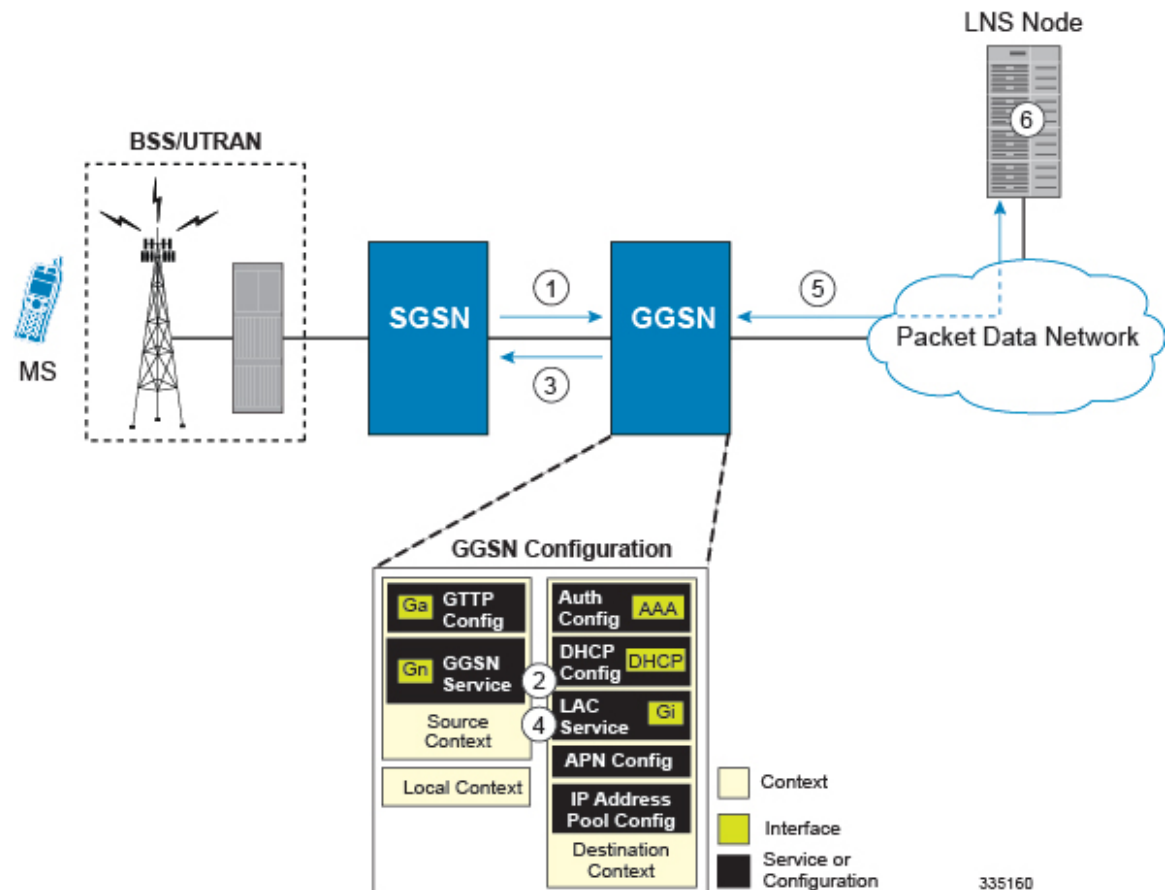
- **Transparent IP:** The APN template's L2TP parameter settings will be applied to the session.
- **Non-transparent IP:** Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.
- **PPP:** The APN template's L2TP parameter settings will be applied and all of the subscriber's PPP packets will be forwarded to the specified LNS.

More detailed information is located in the sections that follow.

Transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 76: Transparent IP PDP Context Call Processing with L2TP Tunneling



- 1 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.

- 2 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber's International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

- 1 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.

- 2 The GGSN passes data received from the MS to a LAC service.

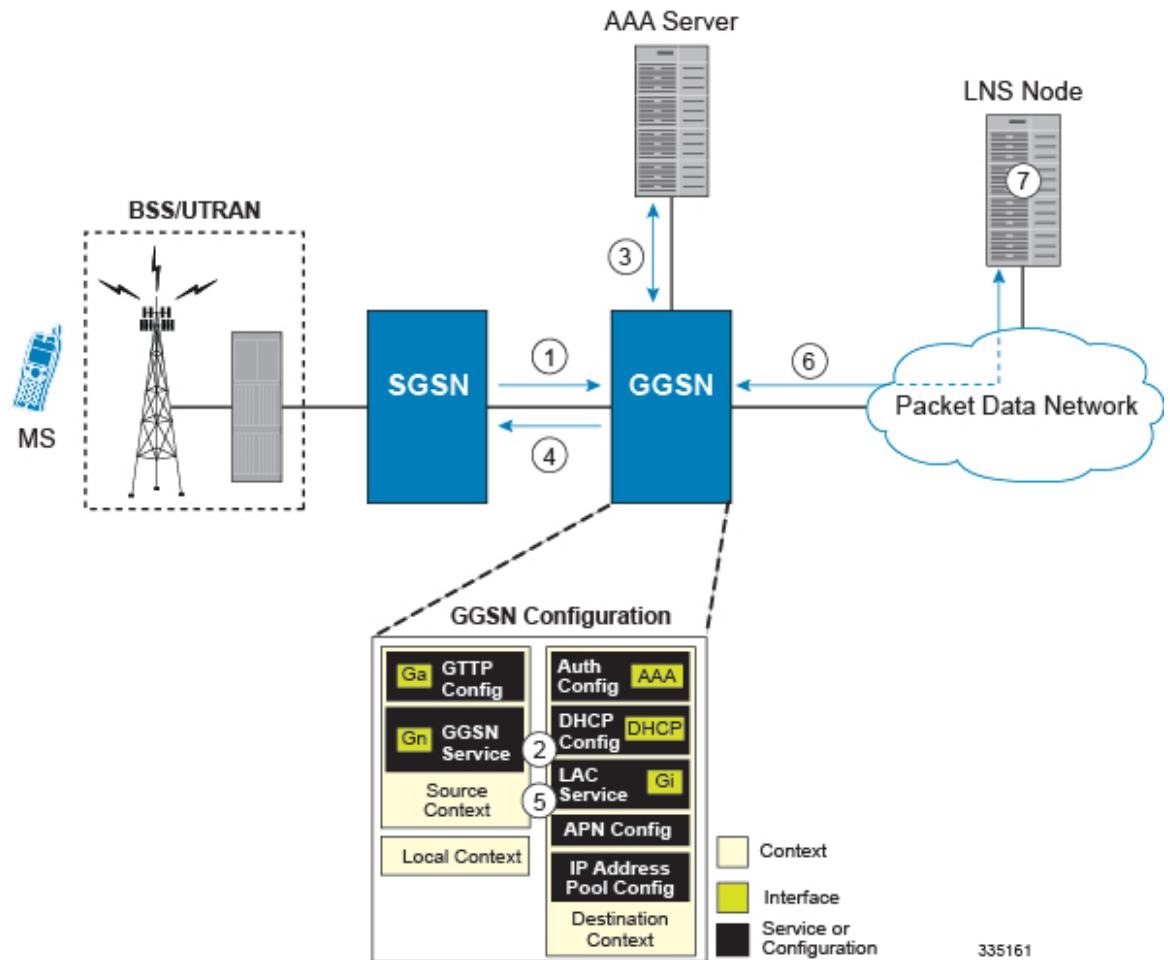
- 3 The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.

- 4 The LNS un-encapsulates the packets and processes them as needed. The processing includes IP address allocation.

Non-transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 77: Non-transparent IP PDP Context Call Processing with L2TP Tunneling



- 1 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 2 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber's username is sent to the peer LNS.

- 3 The GGSN service authenticates the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.

As part of the authentication, the RADIUS server returns an Access-Accept message.

The message may include attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

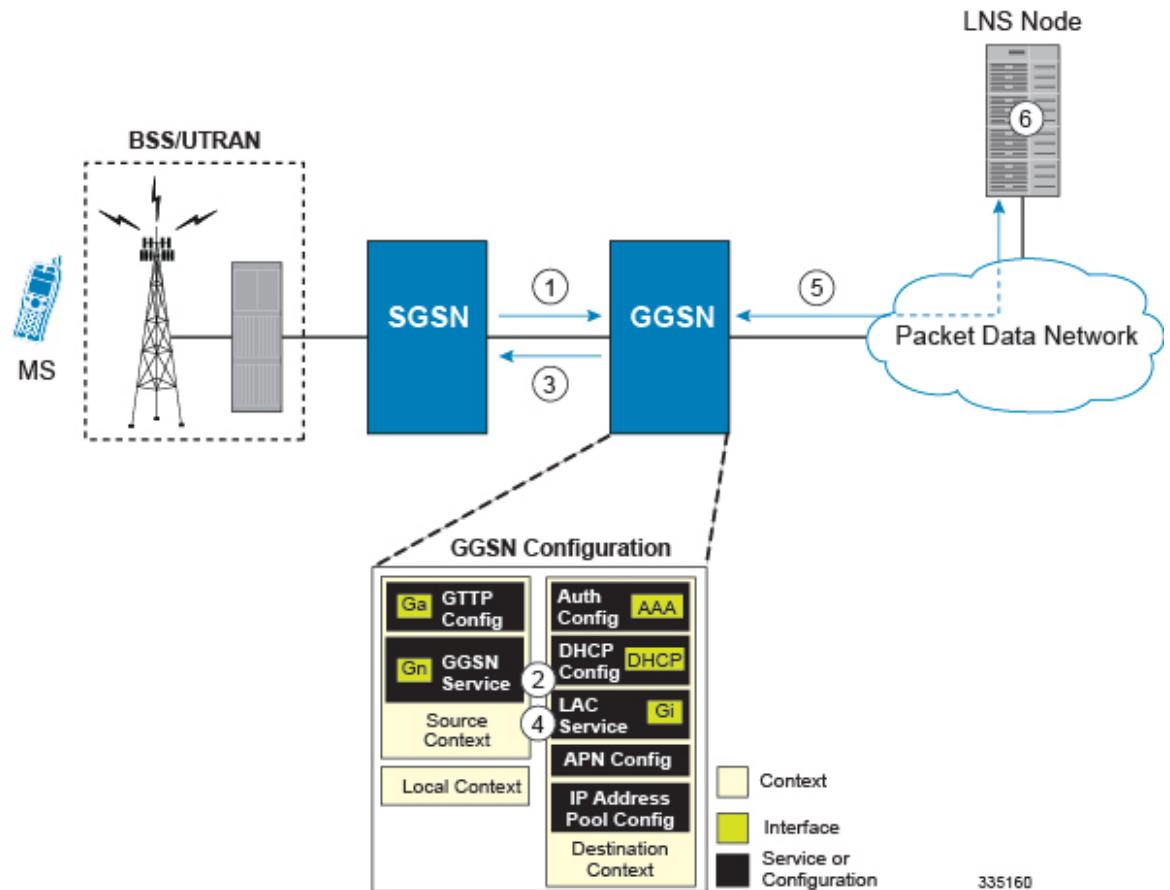
If these attributes are supplied, they take precedence over those specified in the APN template.

- 4 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 5 The GGSN passes data received from the MS to a LAC service.
- 6 The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
- 7 The LNS un-encapsulates the packets and processes them as needed. The processing includes authentication and IP address allocation.

PPP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 78: PPP PDP Context Call Processing with L2TP Tunneling



- 1 A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
- 2 The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured.

Note that L2TP support could also be configured in the subscriber's profile. If the APN is not configured for L2TP tunneling, the system will attempt to authenticate the subscriber. The tunneling parameters in the subscriber's profile would then be used to determine the peer LNS.

- 3 The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
- 4 The GGSN passes the PPP packets received from the MS to a LAC service.

- 5 The LAC service encapsulates the PPP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
- 6 The LNS un-encapsulates the packets and processes them as needed. The processing includes PPP termination, authentication (using the username/password provided by the subscriber), and IP address allocation.

Configuring the GGSN or P-GW to Support L2TP

This section provides a list of the steps required to configure the GGSN or P-GW to support L2TP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



Important

These instructions assume that the system was previously configured to support subscriber data sessions as a GGSN or P-GW.

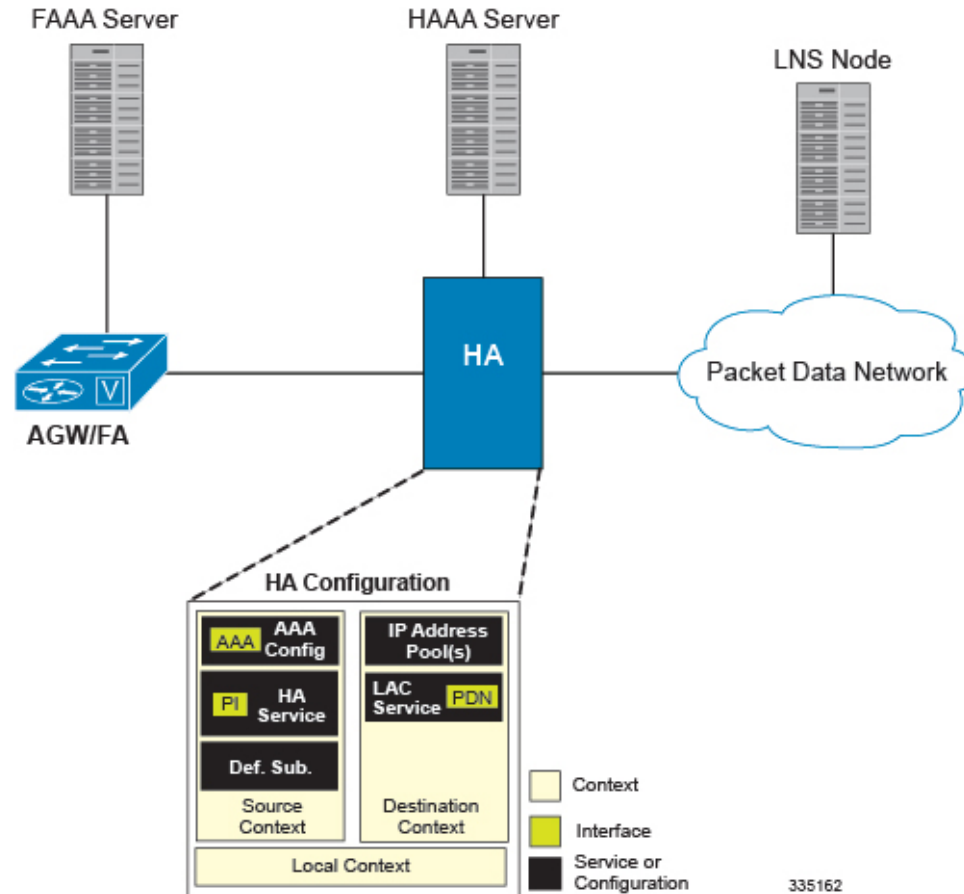
-
- Step 1** Configure the APN template to support L2TP tunneling according to the information and instructions located in the *Modifying APN Templates to Support L2TP* section of this chapter.
- Important** L2TP tunneling can be configured within individual subscriber profiles as opposed/or in addition to configuring support with an APN template. Subscriber profile configuration is described in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.
- Step 2** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Supported LAC Service Configuration for Mobile IP

LAC services can be applied to incoming MIP sessions using attribute-based tunneling. Attribute-based tunneling is used to encapsulate PPP packets for specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

Each LAC service is bound to a single system interface within the same system context. It is recommended that this context be a destination context as displayed in figure below.

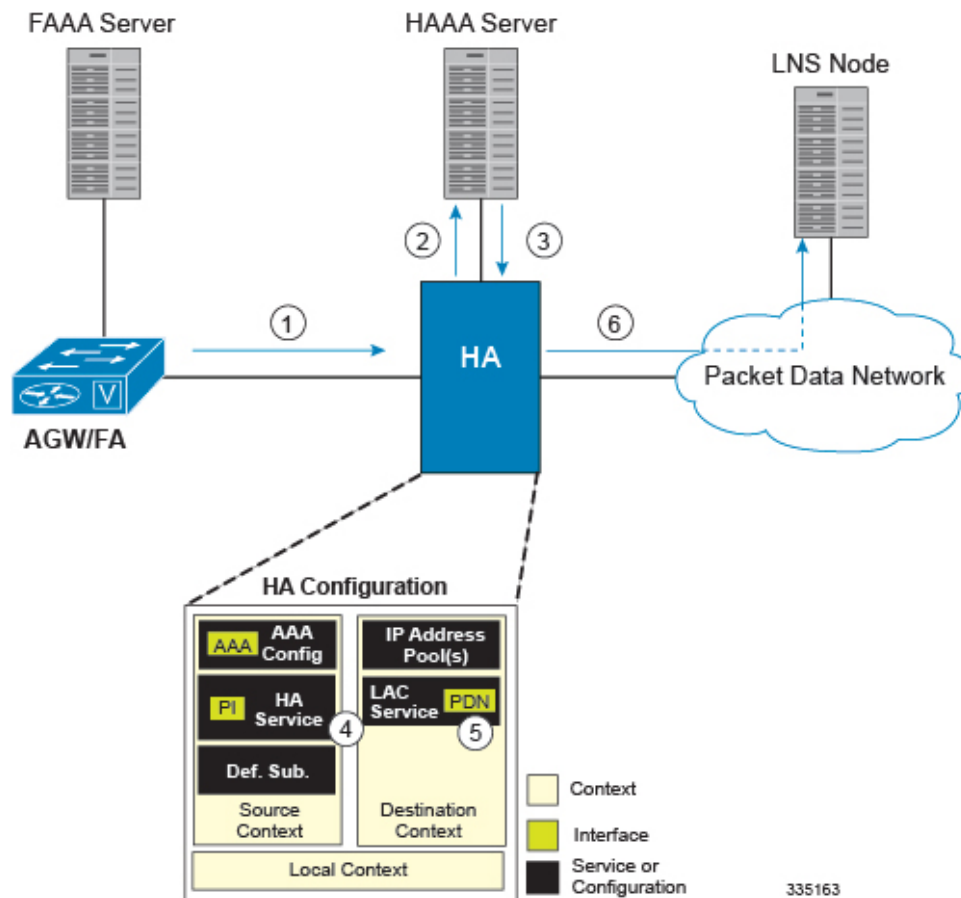
Figure 79: LAC Service Configuration for MIP



How The Attribute-based L2TP Configuration for MIP Works

The following figure and the text that follows describe how Attribute-based tunneling for MIP is performed using the system.

Figure 80: Attribute-based L2TP Session Processing for MIP



- 1 A subscriber session from the FA is received by the HA service over the Pi interface.
- 2 The HA service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
- 3 The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
- 4 The HA service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
- 5 The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
- 6 The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for HA Mobile IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with HA Mobile IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.



Important

These instructions assume that the system was previously configured to support subscriber data sessions as an HA.

-
- Step 1** Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.
- Step 2** Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Configuring Subscriber Profiles for L2TP Support

This section provides information and instructions on the following procedures:

- [RADIUS and Subscriber Profile Attributes Used, on page 595](#)
- [Configuring Local Subscriber Profiles for L2TP Support, on page 597](#)
- [Configuring Local Subscriber, on page 598](#)
- [Verifying the L2TP Configuration, on page 599](#)



Important

Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

RADIUS and Subscriber Profile Attributes Used

Attribute-based L2TP tunneling is supported through the use of attributes configured in subscriber profiles stored either locally on the system or remotely on a RADIUS server. The following table describes the attributes used in support of LAC services. These attributes are contained in the standard and VSA dictionaries.

Table 40: Subscriber Attributes for L2TP Support

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Type	tunnel l2tp	Specifies the type of tunnel to be used for the subscriber session	L2TP
Tunnel-Server-Endpoint	tunnel l2tp peer-address	Specifies the IP address of the peer LNS to connect tunnel to.	IPv4 address in dotted-decimal format, enclosed in quotation marks
Tunnel-Password	tunnel l2tp secret	Specifies the shared secret between the LAC and LNS.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks
Tunnel-Private-Group-ID	tunnel l2tp tunnel-context	Specifies the name of the destination context configured on the system in which the LAC service(s) to be used are located. Important If the LAC service and egress interface are configured in the same context as the core service or HA service, this attribute is not needed.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks
Tunnel-Preference	tunnel l2tp preference	Configures the priority of each peer LNS when multiple LNS nodes are configured. Important This attribute is only used when the loadbalance-tunnel-peers parameter or SN-Tunnel-Load-Balancing attribute configured to prioritized.	Integer from 1 to 65535

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
SN-Tunnel-Load-Balancing	loadbalance-tunnel-peer	A vendor-specific attribute (VSA) used to provides a selection algorithm defining how an LNS node is selected by the RADIUS server when multiple LNS peers are configured within the subscriber profile.	<ul style="list-style-type: none"> • Random - Random LNS selection order, the Tunnel-Preference attribute is not used in determining which LNS to select. • Balanced - LNS selection is sequential balancing the load across all configured LNS nodes, the Tunnel-Preference attribute is not used in determining which LNS to select. • Prioritized - LNS selection is made based on the priority assigned in the Tunnel-Preference attribute.
Client-Endpoint	local-address	<p>Specifies the IP address of a specific LAC service configured on the system that to use to facilitate the subscriber's L2TP session.</p> <p>This attribute is used when multiple LAC services are configured.</p>	IPv4 address in dotted decimal notation. (xxx.xxx.xxx.xxx)

RADIUS Tagging Support

The system supports RADIUS attribute tagging for tunnel attributes. These "tags" organize together multiple attributes into different groups when multiple LNS nodes are defined in the user profile. Tagging is useful to ensure that the system groups all the attributes used for a specific server. If attribute tagging is not supported by your specific RADIUS server, the system implicitly organizes the attributes in the order that they are listed in the access accept packet.

Configuring Local Subscriber Profiles for L2TP Support

This section provides information and instructions for configuring local subscriber profiles on the system to support L2TP.

**Important**

The configuration of RADIUS-based subscriber profiles is not discussed in this document. Please refer to the documentation supplied with your RADIUS server for further information.

**Important**

This section provides the minimum instruction set for configuring local subscriber profile for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to provide L2TP support to subscribers:

-
- Step 1** Configure the "Local" subscriber with L2TP tunnel parameters and the load balancing parameters with action by applying the example configuration in the *Configuring Local Subscriber* section.
- Step 2** Verify your L2TP configuration by following the steps in the *Verifying the L2TP Configuration* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Configuring Local Subscriber

Use the following example to configure the Local subscriber with L2TP tunnel parameters. Optionally you can configure load balancing between multiple LNS servers:

configure

```
context <ctxt_name> [-noconfirm]
  subscriber name <subs_name>
    tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [ encrypted ] secret
    <secret_string> | tunnel-context <context_name> | local-address <local_ip_address> }
    load-balancing { random | balanced | prioritized }
  end
```

Notes:

- <ctxt_name> is the system context in which you wish to configure the subscriber profile.
- <lns_ip_address> is the IP address of LNS server node and <local_ip_address> is the IP address of system which is bound to LAC service.

Verifying the L2TP Configuration

These instructions are used to verify the L2TP configuration.

Verify that your L2TP configurations were configured properly by entering the following command in Exec Mode in specific context:

show subscriber configuration username *user_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes

As with other services supported by the system, values for subscriber profile attributes not returned as part of a RADIUS Access-Accept message can be obtained using the locally configured profile for the subscriber named default. The subscriber profile for default must be configured in the AAA context (i.e. the context in which AAA functionality is configured).

As a time saving feature, L2TP support can be configured for the subscriber named default with no additional configuration for RADIUS-based subscribers. This is especially useful when you have separate source/AAA contexts for specific subscribers.

To configure the profile for the subscriber named default, follow the instructions above for configuring a local subscriber and enter the name default.

Configuring LAC Services



Important

Not all commands, keywords and functions may be available. Functionality is dependent on platform and license(s).

This section provides information and instructions for configuring LAC services on the system allowing it to communicate with peer LNS nodes.



Important

This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

-
- Step 1** Configure the LAC service on system and bind it to an IP address by applying the example configuration in the *Configuring LAC Service* section.
- Step 2** *Optional.* Configure LNS peer information if the Tunnel-Service-Endpoint attribute is not configured in the subscriber profile or PDSN compulsory tunneling is supported by applying the example configuration in the *Configuring LNS Peer* section.
- Step 3** Verify your LAC configuration by following the steps in the Verifying the LAC Service Configuration section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Configuring LAC Service

Use the following example to create the LAC service and bind the service to an IP address:

```
configure
  context <dst_ctxt_name> [-noconfirm]
    lac-service <service_name>
      bind address <ip_address>
    end
```

Notes:

- <dst_ctxt_name> is the destination context where you want to configure the LAC service.

Configuring LNS Peer

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
  context <dst_ctxt_name> [ -noconfirm ]
    lac-service <service_name>
      tunnel selection-key tunnel-server-auth-id
      peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name> {[encrypted]
isakmp-secret <secret> }} [description <text>] [ preference <integer>]
      load-balancing { random | balanced | prioritized }
    end
```

Notes:

- <dst_ctxt_name> is the destination context where the LAC service is configured.

Verifying the LAC Service Configuration

These instructions are used to verify the LAC service configuration.

Verify that your LAC service configurations were configured properly by entering the following command in Exec Mode in specific context:

show lac-service name *service_name*

The output given below is a concise listing of LAC service parameter settings as configured.

```
Service name: vpn1
Context:          ispl
Bind:             Done
Local IP Address: 192.168.2.1
First Retransmission Timeout: 1 (secs)
Max Retransmission Timeout: 8 (secs)
Max Retransmissions: 5
Max Sessions:     500000      Max Tunnels: 32000
Max Sessions Per Tunnel: 512
Data Sequence Numbers: Enabled   Tunnel Authentication: Enabled
Keep-alive interval: 60         Control receive window: 16
Max Tunnel Challenge Length: 16
Proxy LCP Authentication: Enabled
Load Balancing:     Random
Service Status:     Started
Newcall Policy:     None
```

Modifying PDSN Services for L2TP Support

PDSN service modification is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but cannot determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.



Important

This section provides the minimum instruction set for modifying PDSN service for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

-
- Step 1** Modify the PDSN service to support L2TP by associating LAC context and defining tunnel type by applying the example configuration in the *Modifying PDSN Service* section.
- Step 2** Verify your configuration to modify PDSN service by following the steps in the *Verifying the PDSN Service for L2TP Support* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-

Modifying PDSN Service

Use the following example to modify the PDSN service to support L2TP by associating LAC context and defining tunnel type:

```
configure
context <source_ctxt_name> [ -noconfirm ]
pdsn-service <pdsn_service_name>
  ppp tunnel-context <lac_context_name>
  ppp tunnel-type { l2tp | none }
end
```

Notes:

- <source_ctxt_name> is the name of the source context containing the PDSN service, which you want to modify for L2TP support.
- <pdsn_service_name> is the name of the pre-configured PDSN service, which you want to modify for L2TP support.
- <lac_context_name> is typically the destination context where the LAC service is configured.

Verifying the PDSN Service for L2TP Support

These instructions are used to verify the PDSN service configuration.

Verify that your PDSN is configured properly by entering the following command in Exec Mode in specific context:

show pdsn-service name *pdsn_service_name*

The output of this command is a concise listing of PDSN service parameter settings as configured.

Modifying APN Templates to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.



Important

This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

- Step 1** Modify the APN template to support L2TP with LNS server address and other parameters by applying the example configuration in the *Assigning LNS Peer Address in APN Template* section.
- Step 2** Optional. If L2TP will be used to tunnel transparent IP PDP contexts, configure the APN's outbound username and password by applying the example configuration in the *Configuring Outbound Authentication* section.
- Step 3** Verify your APN configuration by following the steps in the *Verifying the APN Configuration* section.
- Step 4** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Assigning LNS Peer Address in APN Template

Use following example to assign LNS server address with APN template:

configure

```
context <dst_ctxt_name> [-noconfirm]
  apn <apn_name>
    tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret <l2tp_secret> ] [ preference
<integer> ] [ tunnel-context <l2tp_context_name> ] [ local-address <local_ip_address> ] [ crypto-map
<map_name> { [ encrypted ] isakmp-secret <crypto_secret> } ]
    end
```

Notes:

- <dst_ctxt_name> is the name of system destination context in which the APN is configured.
- <apn_name> is the name of the pre-configured APN template which you want to modify for the L2TP support.
- <lns_address> is the IP address of LNS server node and <local_ip_address> is the IP address of system which is bound to LAC service.

Configuring Outbound Authentication

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
  context <dst_ctxt_name> [ -noconfirm ]
    apn <apn_name>
      outbound { [ encrypted ] password <pwd> | username <name> }
    end
```

Notes:

- <dst_ctxt_name> is the destination context where APN template is configured.
- <apn_name> is the name of the pre-configured APN template which you want to modify for the L2TP support.

Verifying the APN Configuration

These instructions are used to verify the APN configuration.

Verify that your APN configurations were configured properly by entering the following command in Exec Mode in specific context:

show apn name *apn_name*

The output is a concise listing of APN parameter settings as configured.



CHAPTER 26

L2TP Network Server

This chapter describes the support for Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) functionality on Cisco® ASR 5500 chassis and explains how it is configured. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

The Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

When enabled through the session license and feature use key, LNS functionality is configured as context-level services on the system. LNS services support the termination of L2TP encapsulated tunnels from L2TP Access Concentrators (LACs) in accordance with RFC 2661.



Important

The LNS service uses UDP ports 13660 through 13668 as the source port for receiving packets from the LAC. You can force the LNS to only use the standard L2TP port (UDP Port 1701) with the **single-port-mode** LNS service configuration mode command. Refer to the *Command Line Interface Reference* for more information on this command.

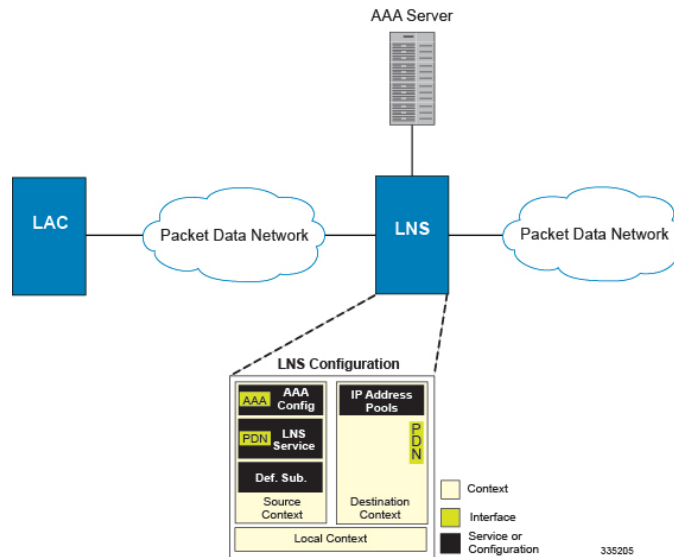
- [LNS Service Operation, page 605](#)
- [Configuring the System to Support LNS Functionality, page 612](#)

LNS Service Operation

As mentioned previously, LNS functionality on the system is configured via context-level services. LNS services can be configured in the same context as other services supported on the system or in its own context. Each context can support multiple LNS services.

One of the most simple configuration that can be implemented on the system to support Simple IP data applications requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

Figure 81: LNS Configuration Example



The source context facilitates the LNS service(s) and the PDN and AAA interfaces. The PDN interface is bound to the LNS service and connects L2TP tunnels and sessions from one or more peer LACs. The source context is also be configured to provide AAA functionality for subscriber sessions. The destination context facilitates the packet data network interface(s) and can optionally be configured with pools of IP addresses for assignment to subscriber sessions.

In this configuration, the LNS service in the source context terminates L2TP tunnels from peer LACs and routes the subscriber session data through the destination context to and from a packet data network such as the Internet or a home network.

Information Required

Prior to configuring the system as shown in figure above, a minimum amount of information is required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 41: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.

Required Information	Description
PDN Interface Configuration	
PDN interface name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>These PDN interfaces facilitates the L2TP tunnels/sessions from the LAC and are configured in the source context.</p>
IP address and subnet	<p>These will be assigned to the PDN interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	<p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the source context and are used to bind logical PDN interfaces.</p>
Gateway IP address	Used when configuring static routes from the PDN interface(s) to a specific network.
LNS service Configuration	
LNS service name	<p>This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the LNS service will be recognized by the system.</p> <p>Multiple names are needed if multiple LNS services will be used.</p> <p>LNS services are configured in the source context.</p>
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.
Maximum number of sessions per tunnel	<p>This defines the maximum number of sessions supported by each tunnel facilitated by the LNS service.</p> <p>The number can be configured to any integer value from 1 to 65535. The default is 65535.</p>

Required Information	Description
Maximum number of tunnels	This defines the maximum number of tunnels supported by the LNS service. The number can be configured to any integer value from 1 to 32000. The default is 32000.
Peer LAC	IP address or network prefix and mask: The IP address of a specific peer LAC for which the LNS service terminates L2TP tunnels. The IP address must be expressed in dotted decimal notation. Multiple peer LACs can be configured. Alternately, to simplify configuration, a group of peer LACs can be specified by entering a network prefix and a mask.
	Secret: The shared secret used by the LNS to authenticate the peer LAC. The secret can be from 1 to 256 alpha and/or numeric characters and is case sensitive.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	

Required Information	Description
RADIUS Authentication server	<p>IP Address:</p> <p>Specifies the IP address of the RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret:</p> <p>The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number:</p> <p>Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>
RADIUS Accounting server	<p>IP Address:</p> <p>Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.</p>
	<p>Shared Secret:</p> <p>The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p>
	<p>UDP Port Number:</p> <p>Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary IP address interface can optionally be configured.
Default Subscriber Configuration	

Required Information	Description
"Default" subscriber's IP context name	<p>Specifies the name of the egress context on the system that facilitates the PDN ports.</p> <p>Important For this configuration, the IP context name should be identical to the name of the destination context.</p>

Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 42: Required Information for Destination Context Configuration

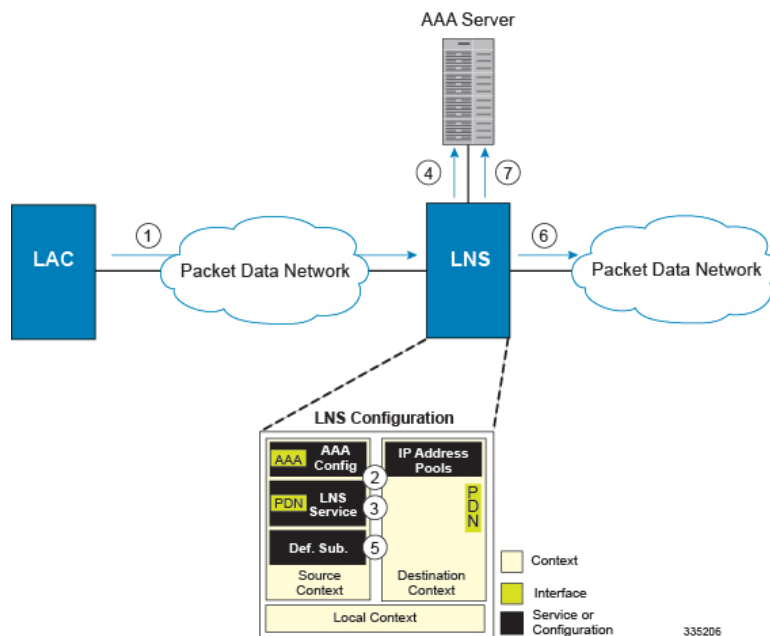
Required Information	Description
Destination context name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.</p> <p>Important For this configuration, the destination context name should not match the domain name of a specific domain.</p>
PDN Interface Configuration	
PDN interface name	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>PDN interfaces are used to connect to a packet network and are configured in the destination context.</p>
IP address and subnet	<p>These will be assigned to the PDN interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description(s)	<p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions will be needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical PDN interfaces.</p>
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	

Required Information	Description
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

How This Configuration Works

The following figure and the text that follows describe how this LNS service configuration with a single source and destination context would be used by the system to terminate an L2TP tunnel.

Figure 82: Call Processing Using a Single Source and Destination Context



- 1 An L2TP tunnel request from a peer LAC is received by the LNS service. The tunnel is to facilitate a subscriber session.
- 2 The LAC and LNS establish the L2TP tunnel according to the procedures defined in RFC 2661. Once the L2TP tunnel is established, subscriber L2TP sessions can be established.
- 3 The LNS service determines which context to use in providing AAA functionality for the subscriber session if authentication is enabled for the LNS service. For more information on this process, refer How the System Selects Contexts in System Administration Guide.

For this example, the result of this process is that LNS service determined that AAA functionality should be provided by the Source context.

- 4 The system communicates with the AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
- 5 Upon successful authentication, the LNS service terminates the subscriber's PPP datagrams from the L2TP session and the system determines which egress context to use for the subscriber session. For more information on egress context selection process, refer *How the System Selects Contexts* in *System Administration Guide*.
The system determines that the egress context is the destination context based on the configuration of either the Default subscriber's ip-context name or from the SN-VPN-NAME or SN1-VPN-NAME attributes that is configured in the subscriber's RADIUS profile.
- 6 Data traffic for the subscriber session is routed through the PDN interface in the Destination context.
- 7 Accounting information for the session is sent to the AAA server over the AAA interface.

Configuring the System to Support LNS Functionality

Many of the procedures required to configure the system to support LNS functionality are provided in the *System Administration Guide*. The *System Administration Guide* provides information and procedures for configuring contexts, interfaces and ports, AAA functionality, and IP address pools on the system.

This section provides information and instructions for configuring LNS services on the system allowing it to communicate with peer LAC nodes.



Important

This section provides the minimum instruction set for configuring an LNS service allowing the system to terminate L2TP tunnels and process data sessions. For more information on commands that configure additional LNS service properties, refer *LNS Configuration Mode Commands* chapter in *Command Line Interface Reference*.

To configure the system to provide access control list facility to subscribers:

-
- | | |
|---------------|---|
| Step 1 | Create the LNS service and bind it to an interface IP address by applying the example configuration in the <i>Creating and Binding LNS Service</i> section. |
| Step 2 | Specify the authentication parameters for LNS service by applying the example configuration in the <i>Configuring Authentication Parameters for LNS Service</i> section. |
| Step 3 | Configure the maximum number of tunnels supported by the LNS service and maximum number of sessions supported per tunnel by applying the example configuration in the <i>Configuring Tunnel and Session Parameters for LNS Service</i> section. |
| Step 4 | Configure peer LACs for the LNS service by applying the example configuration in the <i>Configuring Tunnel and Session Parameters for LNS Service</i> section. |
| Step 5 | <i>Optional.</i> Specify the domain alias designated for the context which the LNS service uses for AAA functionality by applying the example configuration in the <i>Configuring Domain Alias for AAA Subscribers</i> section. |
| Step 6 | Verify your LNS service configuration by following the steps in the <i>Verifying the LNS Service Configuration</i> section. |
| Step 7 | Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration . For additional information on how to verify and save configuration files, refer to the <i>System Administration Guide</i> and the <i>Command Line Interface Reference</i> . |
-

Creating and Binding LNS Service

Use the following example to create the LNS service and bind the IP address to it:

```
configure
  context <dest_ctxt_name> -noconfirm
    lns-service <lns_svc_name> -noconfirm
      bind address <ip_address> [ max-subscribers <max_subscriber> ]
    end
```

Notes:

- LNS service has to be configured in destination context.
- Bind address is the interface address that is to serve as an L2TP PDN interface.
- Multiple addresses on the same IP interface can be bound to different LNS services. However, each address can be bound to only one LNS service. In addition, the LNS service can not be bound to the same interface as other services such as a LAC service.

Configuring Authentication Parameters for LNS Service

Use the following example to authentication parameters for LNS service:

```
configure
  context <dest_ctxt_name>
    lns-service <lns_svc_name>
      authentication { { [ allow-noauth | chap <pref> | mschap <pref> | | pap <pref> ] } }
    msid-auth }
  end
```

Note:

- For more information on authentication procedure and priorities, refer **authentication** command section in LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Tunnel and Session Parameters for LNS Service

Use the following example to configure the tunnel and session parameters for LNS service:

```
configure
  context <dest_ctxt_name>
    lns-service <lns_svc_name>
      max-tunnel <max_tunnels>
      max-session-per-tunnel <max_sessions>
    end
```

Note:

- For more information on tunnel and session related parameters, refer LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Peer LAC servers for LNS Service

Use the following example to configure the peer LAC servers for LNS service:

```
configure
  context <dest_ctxt_name>
    lns-service <lns_svc_name>
      peer-lac { <lac_ip_address> | <ip_address>/<mask> } [ encrypted ] secret
    <secret_string> [ description <desc_text> ]
  end
```

Note:

- Multiple LACs can be configured with this command. For more information, refer LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Domain Alias for AAA Subscribers

Use the following example to create the LNS service and bind the IP address to it:

```
configure
  context <dest_ctxt_name> -noconfirm
    lns-service <lns_svc_name> -noconfirm
      nai-construct domain <domain_alias>
    end
```

Notes:

- If this command is enabled, an NAI is constructed for the subscriber in the event that their mobile node does not negotiate CHAP, PAP, or MSCHAP.
- If this option is selected, no further attempts are made to authenticate the user. Instead, the constructed NAI is used for accounting purposes.

**Important**

This command should only be used if the LNS service is configured to allow "no authentication" using the **authentication allow-noauth** command.

Verifying the LNS Service Configuration

These instructions are used to verify the LNS service configuration.

Verify that your LNS service configuration by entering the following command in Exec Mode:

show lns-service name *service_name*

The output of this command displays the configuration of the LNS service and should appear similar to that shown below.

```
Service name: testlns
Context: test
Bind: Not Done
Local IP Address: 0.0.0.0
First Retransmission Timeout: 1 (secs)
Max Retransmission Timeout: 8 (secs)
Max Retransmissions: 5
Setup Timeout: 60 (secs)
Max Sessions: 500000 Max Tunnels: 32000
Max Sessions Per Tunnel: 65535
Keep-alive Interval: 60 Control Receive Window: 16
Data Sequence Numbers: Enabled
Tunnel Authentication: Enabled
Tunnel Switching: Enabled
Max Tunnel Challenge Length: 16
PPP Authentication: CHAP 1 PAP 2
Allow Noauthentication: Disabled MSID Authentication: Disabled
No NAI Construct Domain defined
No Default Subscriber defined
IP Src Violation Reneg Limit: 5
IP Src Violation Drop Limit: 10
IP Src Violation Period: 120 (secs)
Service Status: Not started
Newcall Policy: None
```




Mobile IP Registration Revocation

This chapter describes Registration Revocation for Mobile-IP and Proxy Mobile-IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in this administration guide before using the procedures in this chapter.



Important

This license is enabled by default; however, not all features are supported on all platforms and other licenses may be required for full functionality as described in this chapter.

This chapter includes the following topics:

- [Overview, page 617](#)
- [Configuring Registration Revocation, page 618](#)

Overview

Registration Revocation is a general mechanism whereby either the HA or the FA providing Mobile IP functionality to the same mobile node can notify the other mobility agent of the termination of a binding. This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

Mobile IP Registration Revocation can be triggered at the FA by any of the following:

- Session terminated with mobile node for whatever reason
- Session renegotiation
- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)

**Important**

Registration Revocation functionality is also supported for Proxy Mobile IP. However, only the HA can initiate the revocation for Proxy-MIP calls.

Mobile IP Registration Revocation can be triggered at the HA by any of the following:

- Administrative clearing of calls
- Inter-Access Gateway handoff. This releases the binding at the previous access gateway/FA
- Session Manager software task outage resulting in the loss of FA sessions (for sessions that could not be recovered)
- Session Idle timer expiry (when configured to send Revocation)
- Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested, etc.)

The FA and the HA negotiate Registration Revocation support when establishing a Mobile IP call. Revocation support is indicated to the Mobile Node (MN) from the FA by setting the 'X' bit in the Agent Advertisement to MN. However the MN is not involved in negotiating the Revocation for a call or in the Revocation process. It only gets notified about it. The X bit in the Agent Advertisements is just a hint to the MN that revocation is supported at the FA but is not a guarantee that it can be negotiated with the HA

At the FA, if revocation is enabled and a FA-HA SPI is configured, the Revocation Support extension is appended to the RRQ received from the MN and protected by the FA-HA Authentication Extension. At the HA, if the RRQ is accepted, and the HA supports revocation, the HA responds with an RRP that includes the Revocation Support extension. Revocation support is considered to be negotiated for a binding when both sides have included a Revocation Support Extension during a successful registration exchange.

**Important**

The Revocation Support Extension in the RRQ or RRP must be protected by the FA-HA Authentication Extension. Therefore, an FA-HA SPI must be configured at the FA and the HA for this to succeed.

If revocation is enabled at the FA, but an FA-HA SPI is not configured at the FA for a certain HA, then FA does not send Revocation Support Extension for a call to that HA. Therefore, the call may come up without Revocation support negotiated.

If the HA receives an RRQ with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with "FA Failed Authentication" error.

If the FA receives a RRP with Revocation Support Extension, but not protected by FA-HA Auth Extension, it will be rejected with "HA Failed Authentication" error.

Also note that Revocation support extension is included in the initial, renewal or handoff RRQ/RRP messages. The Revocation extension is not included in a Deregistration RRQ from the FA and the HA will ignore them in any Deregistration RRQs received.

Configuring Registration Revocation

Support for MIP Registration Revocation requires the following configurations:

- **FA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.

- **HA service(s):** Registration Revocation must be enabled and operational parameters optionally configured.

**Important**

These instructions assume that the system was previously configured to support subscriber data sessions for a core network service with FA and/or an HA according to the instructions described in the respective product Administration Guide.

**Important**

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring FA Services

Configure FA services to support MIP Registration Revocation by applying the following example configuration:

```
configure
context <context_name>
  fa-service <fa_service_name>
    revocation enable
    revocation max-retransmission <number>
    revocation retransmission-timeout <time>
  end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring HA Services

Configure HA services to support MIP Registration Revocation by applying the following example configuration:

```
configure
context <context_name>
  ha-service <ha_service_name>
    revocation enable
    revocation max-retransmission <number>
    revocation retransmission-timeout <time>
  end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



Multimedia Broadcast and Multicast Service

This chapter provides information on Multimedia Broadcast and Multicast Service (MBMS) functionality on GGSN. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

The features described in this chapter are only available if you have purchased and installed MBMS feature support license on your chassis.

- [Introduction, page 621](#)
- [Supported Standards, page 623](#)
- [Supported Networks and Platforms, page 623](#)
- [Services and Application in MBMS, page 623](#)
- [How MBMS Works, page 625](#)
- [MBMS Configuration, page 627](#)
- [Save the Configuration, page 629](#)
- [Managing Your Configuration, page 629](#)
- [Gathering MBMS Statistics, page 631](#)

Introduction

MBMS is an IP datacast type of service in GSM and UMTS cellular network. It eliminates unnecessary replication of data on UMTS wireless networks by transmitting a single stream of data to multiple users. By delivering a single, unidirectional data stream to many subscribers, MBMS makes more efficient use of wireless network resources than traditional point to point connections.

MBMS is a solution for transferring light video and audio clips with a suitable method for mass communications.

MBMS functionality on the system is provided by an existing GGSN service and is enabled by a valid services license.

The main features supported by the Multimedia Broadcast & Multicast Services are:

- Individual user network control functions and provide forward MBMS user data to SGSN



Important

The Cisco chassis supports 225 downlink SGSNs per MBMS Bearer Service through NPU assisted data flow processing. NPU assisted data processing is available on the systems with release 8.1 or later only.

- Support for intra-GGSN and inter-GGSN mobility procedures
- Generate charging data per multicast service for each user for both prepaid and post paid subscribers.
- Multicast proxy-host functionality
- Support for MBMS-specific Gmb messages
- Authentication of MBMS flow-ids using a MBMS controller
- Establishment and tear-down of MBMS bearer paths using the multicast framework
- Support for framing HDLC-like and segment based framing
- Accounting for the MBMS flows to charge the originator of the content

This service provides two mode of operations:

- MBMS Broadcast Mode
- MBMS Multicast Mode

A broadcast mode is a unidirectional point-to-multipoint service in which data is transmitted from a single source to multiple terminals (UE/MS) in the associated broadcast service area/cell area. The transmitted data can be text to light multimedia services (Audio, Video etc). On the other hand multicast mode is a unidirectional point-to-multipoint service in which data is transmitted from a single source to a pre-defined multicast group of users that are subscribed to the specific multicast service and have joined the multicast group in the associated multicast service area.

The following figure shows the reference architecture of MBMS service in UMTS network.

The GGSN provides the following functionality to perform MBMS services:

- serves as an entry point for IP multicast traffic as MBMS data. It provides establishment of bearer plan and tear-down of the established bearer plan upon notification from the BM-SC.
- provides functionality to receive MBMS specific IP multicast traffic and to route this data to the proper GTP tunnels set-up as part of the MBMS bearer service.
- provides features, that are not exclusive to MBMS, for the MBMS bearer service, like charging data collection, flow-based charging, optional message screening etc.

MBMS is able to use NPU assisted MBMS data flow processing on chassis so that system can relieve the Session Manager to provide better performance and processing. Currently with NPU assisted data processing, the Cisco chassis can support 225 SGSNs per MBMS Bearer Service for downlink of MBMS data.

Supported Standards

Support for the following standards and requests for comments (Rafts) have been added with the MBMS functionality:

- 3GPP TS 22.146: Multimedia Broadcast/Multicast Service; Stage 1 (Release 6)
- 3GPP TS 22.246: MBMS user services; Stage 1 (Release 6)
- 3GPP TS 23.246: MBMS; Architecture and functional description (Release 6)
- 3GPP TS 26.346: MBMS; Protocols and codecs (Release 6)
- 3GPP TS 33.246: Security of Multimedia Broadcast/Multicast Service
- 3GPP TS 32.251: Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.273: Telecommunication management; Charging management; Multimedia Broadcast and Multicast Service (MBMS) charging
- RFC 3588, Diameter Base Protocol

Supported Networks and Platforms

This feature supports all Cisco chassis running StarOS Release 8.0 or later with GGSN service for the core network services.

License Information



Important

Use of MBMS feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license

Services and Application in MBMS

MBMS service can be used as an enabler for various data streaming services. Compared to traditional broadcast services like cell broadcast, MBMS provides multimedia capabilities with relatively high data rates and considerably greater multimedia capabilities.

Some of the applications for MBMS are:

- News clips
- Audio streams
- Combined audio and picture/video clips
- Video distribution services, either via streaming, carousel, or download methods
- Localized services like tourist information, weather alerts etc.

- Content distribution
- Game delivery

The charging of the MBMS bearer service can be done based on events, content, or flows.

MBMS provides the authentication, key distribution, and data protection for the multicast service users.

MBMS References and Entities

Following are the major components and entities required for MBMS service.

Gmb Reference

The Gmb reference point handles the broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages.

MBMS bearer service specific Gmb signaling includes:

- MBMS bearer context establishment by GGSN and registering of GGSN at BM-SC.
- Release of MBMS bearer context at GGSN and de-registration of GGSN from the BM-SC.
- Session start/stop indication from BM-SC to GGSN including session attributes like QoS or MBMS service area.

User specific Gmb signaling includes:

- BM-SC authorization of user specific MBMS multicast service activation at the GGSN.
- Reporting of successful user specific MBMS multicast service activation by GGSN to BM-SC to synchronize the BM-SC UE MBMS context and charging with the MBMS UE contexts in GGSN.
- Reporting of release or deactivation of user specific MBMS multicast service activation by GGSN to BM-SC to synchronize the BM-SC UE MBMS context and charging with the MBMS UE contexts in GGSN.
- BM-SC initiated deactivation of user specific MBMS bearer service when the MBMS user service is terminated.

MBMS UE Context

A MBMS UE context is defined per UE. Session Manager assign a separate context structure for a MBMS UE Context.

Session Manager maintains the following information as part of MBMS UE Context:

- IP multicast address: IP multicast address identifying an MBMS bearer that the UE has joined.
- APN: Access Point Name on which this IP multicast address is defined.
- SGSN address: The IP address of SGSN
- IMSI: IMSI identifying the user.
- TEID for Control Plane: The Tunnel Endpoint Identifier for the control plane between SGSN and GGSN.

- MBMS NSAPI: Network layer Service Access Point Identifier which identifies an MBMS UE Context.

**Important**

For capacity and resource purpose one MBMS UE context is equal to one PDP context.

MBMS Bearer Context

The MBMS bearer context is created in the SGSN and GGSN for each provisioned MBMS service. This is created when the first MS requests for this service or when a downstream node requests it. Once created, an MBMS context can be in two states:

- Active - is the state in which network resources are required for the transfer of MBMS data.
- Standby - is the state in which no network resources are required.

The MBMS Bearer Context contains all information describing a particular MBMS bearer service and is created in each node involved in the delivery of the MBMS data.

Broadcast Multicast Service Center (BM-SC)

The BM-SC includes functions for MBMS user service provisioning and delivery. It serves as an entry point for content provider MBMS transmissions, used to authorize and initiate MBMS Bearer Services within the PLMN. It can also be used to schedule and deliver MBMS transmissions.

The BM-SC consists of five sub-functions:

- Membership function
- Session and Transmission function
- Proxy and Transport function
- Service Announcement function
- Security function.

BM-SC is a functional entity and must exist for each MBMS User Service.

How MBMS Works

The Multimedia Broadcast Multicast System provides two types of service provisioning; broadcast and multicast modes. This section describes the procedure of these modes.

MBMS Broadcast Mode

The broadcast mode provides unidirectional point-to-multipoint type transmission of multimedia data from a single source to all users that found in a defined broadcast service area. This mode uses radio resources efficiently, since the data is transmitted over a common channel.

MBMS data transmission adapts to the suitable RAN capabilities, depending on the availability of radio resources too. If needed, the bit rate of MBMS data may be varied in order to optimized radio resources.

The following figure shows the basic outline of broadcast mode procedure of an MBMS service in order to broadcast MBMS data within the defined broadcast service area via a packet switched core network.

The broadcast service may include one or more successive broadcast sessions. The user can control the enabling or disabling of the MBMS broadcast mode service.

MBMS Broadcast Mode Procedure

The MBMS performs following steps for broadcast mode user service:

-
- | | |
|---------------|---|
| Step 1 | Service Announcement: Through the service announcement mechanisms, like SMS, WAP, users informed about the available MBMS services. |
| Step 2 | Session Start: This is the phase where BM-SC has data to send and this triggers establishment of network resources for data transfer irrespective of whether a given user has activated the service or not. |
| Step 3 | MBMS Notification: Notifies the MS of a impending MBMS data transfer. |
| Step 4 | Data Transfer: It is the phase when MBMS data are transferred to the UEs. |
| Step 5 | Session Stop: In this phase, the BM-SC determines that it has no more data to send for a time period and so the network resources can be released. |
-

MBMS Multicast Mode

The multicast mode provides unidirectional point-to-multipoint type transmission of multimedia data from a single content source to a group of subscribers that subscribed to specific multicast service separately. The basic difference between broadcast and multicast modes is that the user does not need to subscribe in each broadcast service separately, whereas in multicast mode the services can be ordered separately. The subscription and group joining for the multicast mode service can be done by the operator, user, or a separate service provider.

Like broadcast mode the multicast mode allows the unidirectional point-to-multipoint transmission of multimedia data within the multicast service area. The multicast mode uses radio resources in efficient way by using common radio channel as in broadcast mode. Data is transmitted over the multicast service area as defined by the network operator.

The multicast mode provides the flexibility for the network to selectively transmit to those cells within the multicast service area that contains members of a multicast group.

The following figure shows the basic outline of multicast mode procedure of an MBMS service in order to multicast MBMS data within the defined multicast service area via a packet switched core network.

A multicast service might consist of a single on-going session or may include several simultaneous multicast sessions over an extended period of time.

Some examples of multicast mode service are:

- transmission of sports video clips to subscribers on a charging basis
- transmission of news, movie, song, and audio clips to subscribed users on a charging basis

MBMS Multicast Mode Procedure

The MBMS performs following steps for multicast mode user service:

-
- | | |
|---------------|--|
| Step 1 | Subscription: Establishes the relationship between the user and the service provider, which allows the user to receive the related MBMS multicast service. |
| Step 2 | Service Announcement: Through the service announcement mechanisms like, SMS, WAP, users shall be informed about the available MBMS services. |
| Step 3 | Joining: This is the process by which a subscriber joins a multicast group, i.e. the user indicates to the network that he/she wants to receive Multicast mode data of a specific MBMS bearer service. |
| Step 4 | Session Start: This is the phase where BM-SC is ready to send data and this triggers establishment of network resources for data transfer irrespective of whether a given user has activated the service or not. |
| Step 5 | MBMS Notification: Notifies the MS of a impending MBMS data transfer. |
| Step 6 | Data Transfer: It is the phase when MBMS data are transferred to the UEs. |
| Step 7 | Session Stop: In this phase, the BM-SC determines that it has no more data to send for a time period and so the network resources can be released. |
| Step 8 | Leaving: In this phase, the user leaves a MBMS group through an Internet Group Management Protocol (IGMP) Leave message. |
-

MBMS Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system with MBMS user service in GGSN services.



Important

These instructions assume that you have already configured the GGSN/SGSN system level configuration as described in network function *Administration Guide*.

To configure the system to perform Multimedia Broadcast and Multicast service:

-
- | | |
|---------------|---|
| Step 1 | Configure the BM-SC profile in a context by applying the example configurations presented in the <i>BMSC Profile Configuration</i> section. |
| Step 2 | Configure the MBMS charging parameters in GTPP Server Group Configuration mode by applying the example configurations presented in the <i>MBMS GTPP Configuration</i> section. |
| Step 3 | Configure the MBMS accounting, supported contexts, timeout parameters, and BMSC profile association with APN in APN configuration mode by applying the example configurations presented in the <i>MBMS APN Configuration</i> section. |
| Step 4 | Enable the MBMS user service provisioning mode in GGSN and configure the number of MBMS UE and MBMS bearer context in GGSN configuration mode by applying the example configurations presented in the <i>MBMS Provisioning</i> section. |
| Step 5 | Save the changes to system configuration by applying the example configuration found in <i>Verifying and Saving Your Configuration</i> chapter. |
| Step 6 | Verify configuration of MBMS service related parameters by applying the commands provided in the <i>Managing Your Configuration</i> section of this chapter. |
-

BMSC Profile Configuration

This section provides the configuration example to configure the BM-SC profile in a context:

```
configure
context <vpn_context_name> [ -noconfirm ]
bm-sc-profile name <profile_name> [ -noconfirm ]
default gmb diameter dictionary
gmb diameter endpoint <endpoint_name>
gmb diameter peer-select peer <peer_name> [ realm <realm_name> ] [ secondary-peer
<sec_peer_name> [ realm <sec_realm_name> ]]
default gmb user-data mode-preference
end
```

MBMS GTPP Configuration

This section provides the configuration example to configure the GTPP server parameters in GTPP group configuration mode for MBMS charging:

```
configure
context <vpn_context_name> [ -noconfirm ]
gtp group default
gtp mbms buckets <cc_bucket>
gtp mbms interval <duration_sec>
gtp mbms tariff time1 <mins> <hours> [ time2 <mins> <hours> ]
gtp mbms volume <download_bytes>
end
```


MBMS APN Configuration

This section provides the configuration example to enable the BM-SC profile for an APN and to configure the MBMS accounting, supported contexts, and timeout parameters in APN configuration mode:

```
configure
context <vpn_context_name>
apn <apn_name> [ -noconfirm ]
mbms bmsc-profile name <profile_name>
accounting mode gtp
default mbms bearer timeout { absolute | idle }
default mbms ue timeout absolute
end
```

MBMS Provisioning

This section provides the configuration example for provisioning of MBMS service mode for a GGSN service and associating the MBMS policy for multicast broadcast within the GGSN service in GGSN service configuration mode:

```
configure
context <vpn_context_name>
ggsn-service <ggsn_service_name>

mbms policy multicast broadcast
end
```

Save the Configuration

To save changes made to the system configuration for this service, refer *Verifying and Saving Your Configuration* chapter.

Managing Your Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file as described in *Saving Your Configuration* chapter of this guide and also to retrieve errors and warnings within an active configuration for a service.



Important

All commands listed here are under Exec mode. Not all commands are available on all platforms.

Output descriptions for most of the commands are located in *Command Line Interface Reference*.

To do this:	Enter this command:
View Administrative Information	
Display Current Administrative User Access	

To do this:	Enter this command:
View a list of all administrative users currently logged on to the system	show administrators
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	show administrators session id
View information pertaining to local-user administrative accounts configured for the system	show local-user verbose
View statistics for local-user administrative accounts	show local-user statistics verbose
View information pertaining to your CLI session	show cli
Determining the System's Uptime	
View the system's uptime (time since last reboot)	show system uptime
View the Status of Configured NTP Servers	
View the status of the configured NTP servers	show ntp status
View the Statistics of Broadcast Multicast service	
View the full information of all broadcast-multicast service session	show multicast-sessions full all
View the status of all broadcast multicast-service session	show session in-progress
View all session for broadcast-multicast service	show multicast-sessions all
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	show subscribers all
View information for a specific subscriber	show subscribers full username <user_name>
View the MBMS Related Information	
Display Configured MBMS service	
View the configuration of a context	show configuration context <vpn_ctxt_name>
View configuration errors for GGSN service	show configuration errors section ggsn-service [verbose] [{grep <grep_options> more }]
Display BM-SC server Information	show bmsc servers

Gathering MBMS Statistics

The following table lists the commands that can be used to gather the statistics for MBMS.



Important

All commands listed here are under Exec mode. For more information on these commands, refer *Executive Mode Commands* chapter in *Command Line Interface Reference*.

Table 43: Gathering Statistics

Statistics Wanted	Action to Perform	Information to Look For
Gmb interface statistics for APN and BM-SC profile	At the Exec Mode prompt, enter the following command: show gmb statistics [apn <apn_name>] [bmsc-profile <bmsc_profile_name>] [verbose]	The output of this command displays the statistics about the Gmb interface session for MBMS on an APN.
Detailed MBMS bearer service statistics	At the Exec Mode prompt, enter the following command: show mbms bearer-service [mcast-address <mcast_address>] [apn <apn_name>] [bmsc-profile <bmsc_profile_name>] [service-type { multicast broadcast }] [summary full] [all]	The output of this command displays the MBMS bearer service statistics.
Detailed statistics of MBMS multicast sessions	At the Exec Mode prompt, enter the following command: show multicast-sessions	The output of this command displays the detailed statistics of MBMS multicast session running on system.



Multi-Protocol Label Switching (MPLS) Support

This chapter describes the system's support for BGP/MPLS VPN and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on specific systems. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in the respective product administration guide, before using the procedures in this chapter.

When enabled through a feature license key, the system supports MPLS to provide a VPN connectivity from the system to the corporate's network.



Important

This release provides BGP/MPLS VPN for directly connected PE routers only.

MP-BGP is used to negotiate the routes and segregate the traffic for the VPNs. The network node learns the VPN routes from the connected Provider Edge (PE), while the PE populates its routing table with the routes provided by the network functions.

- [Overview, page 633](#)
- [Supported Standards, page 635](#)
- [Supported Networks and Platforms, page 636](#)
- [Licenses, page 636](#)
- [Benefits, page 636](#)
- [Configuring BGP/MPLS VPN with Static Labels, page 636](#)
- [Configuring BGP/MPLS VPN with Dynamic Labels, page 639](#)

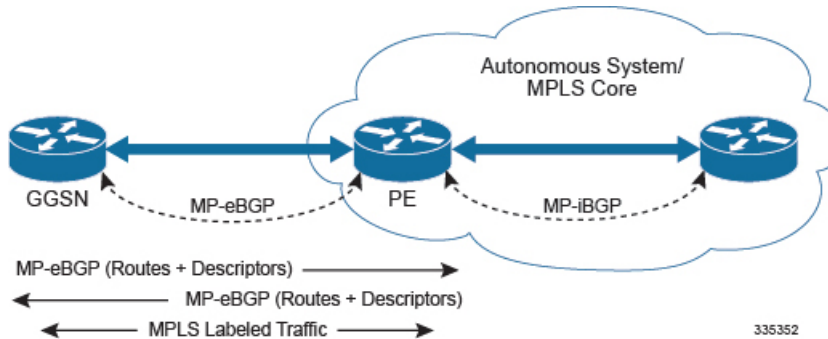
Overview

As seen in the following scenario, the chassis can be deployed as a router while supporting BGP/MPLS-VPN in a network.

- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Provider Edge (PE)
- Chassis as MPLS-Customer Edge (MPLS-CE) connecting to Autonomous System Border Router (ASBR)

Chassis as MPLS-CE Connecting to PE

Figure 86: Chassis as MPLS-CE Connected to PE



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to the [Configuring BGP/MPLS VPN with Static Labels, on page 636](#) section and refer to [Configuring BGP/MPLS VPN with Static Labels, on page 636](#) for dynamic label configuration.

The system is in a separate autonomous system (AS) from the Provider Edge (PE). It communicates with the PE and all VPN routes are exchanged over MP-BGP. Routes belonging to different VPNs are logically separated, using separate virtual route forwarding tables (VRFs).

Routes for each VPN are advertised as VPN-IPv4 routes, where route distinguishers are prepended to regular IPv4 routes to allow them to be unique within the routing table. Route targets added to the BGP extended community attributes identify different VPN address spaces. The particular upstream BGP peer routing domain (VPN), from which a route is to be imported by the downstream peer into an appropriate VRF, is identified with an extended community in the advertised NLRI.

A unique label is also received or advertised for every VPN route.

The Customer Edge (CE) also advertises routes to the PE using NRIs that include route distinguishers to differentiate VPNs, an extended community to identify VRFs, and a MPLS-label, which will later be used to forward data traffic.

There is a single MPLS-capable link between the CE and the PE. MP-BGP communicates across this link as a TCP session over IP. Data packets are sent bidirectionally as MPLS encapsulated packets.

This solution does not use any MPLS protocols. The MPLS label corresponding to the immediate upstream neighbor can be statically configured on the downstream router, and similarly in the reverse direction.

When forwarding subscriber packets in the upstream direction to the PE, the CE encapsulates packets with MPLS headers that identify the upstream VRF (the label sent with the NLRI) and the immediate next hop. When the PE receives a packet it swaps the label and forward.

The CE does not run any MPLS protocol (LDP or RSVP-TE).

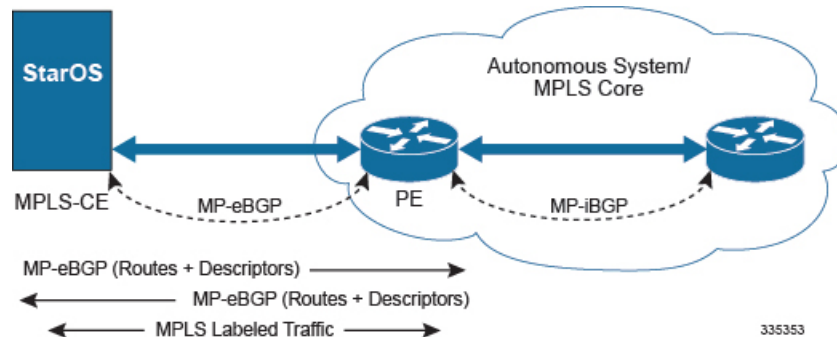
When receiving data packets in the downstream direction from the PE, the label is checked to identify the destination VRF. Then the packet is de-encapsulated into an IP packet and sent to the session subsystem for processing.



Important MPLS ping/trace route debugging facilities are not supported.

Chassis as MPLS-CE Connected to ASBR

Figure 87: Chassis as MPLS-CE Connected to ASBR



The system in this scenario uses static/dynamic MPLS labels for ingress and egress traffic. For configuration information on static label, refer to [Configuring BGP/MPLS VPN with Static Labels](#), on page 636 and refer to [Configuring BGP/MPLS VPN with Dynamic Labels](#), on page 639 for dynamic label configuration.

This scenario differs from the MPLS-CE with PE scenario in terms of peer functionality even though MPLS-CE functionality does not change. Like the MPLS-CE with PE scenario, MPLS-CE system maintains VRF routes in various VRFs and exchanges route information with peer over MP-eBGP session.

The peer in this scenario is not a PE router but an Autonomous System Border Router (ASBR). The ASBR does not need to maintain any VRF configuration. The PE routers use iBGP to redistribute labeled VPN-IPv4 routes either to an ASBR or to a route reflector (of which the ASBR is a client). The ASBR then uses the eBGP to redistribute those labeled VPN-IPv4 routes to an MPLS-CE in another AS. Because of the eBGP connection, the ASBR changes the next-hop and labels the routes learned from the iBGP peers before advertising to the MPLS-CE. The MPLS-CE is directly connected to the eBGP peering and uses only the MP-eBGP to advertise and learn routes. The MPLS-CE pushes/pops a single label to/from the ASBR, which is learned over the MP-eBGP connection. This scenario avoids the configuration of VRFs on the PE, which have already been configured on the MPLS-CE.

Engineering Rules

- Up to 5,000 "host routes" spread across multiple VRFs per BGP process. Limited to 6,000 pool routes per chassis.
- Up to 2,048 VRFs per chassis.

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- RFC 4364, BGP/MPLS IP VPNs
- RFC 3032, MPLS Label Stack Encoding

**Important**

One or more sections of above mentioned IETF are partially supported for this feature. For more information on Statement of Compliance, contact your Cisco account representative.

Supported Networks and Platforms

This feature supports all ASR5500 platforms with StarOS Release 9.0 or later running with network function services.

Licenses

Multi-protocol label switching (MPLS) is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Benefits

MPLS provides networks with a more efficient way to manage applications and move information between locations. MPLS prioritizes network traffic, so administrators can specify which applications should move across the network ahead of others.

Configuring BGP/MPLS VPN with Static Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with static MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.

**Important**

The feature described in this chapter is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

**Important**

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

To configure the system for BGP/MPLS VPN:

-
- Step 1** Create a VRF on the router and assign a VRF name by applying the example configuration in [Create VRF with Route-distinguisher and Route-target](#), on page 637.
 - Step 2** Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in [Set Neighbors and Enable VPNv4 Route Exchange](#), on page 637.
 - Step 3** Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in [Configure Address Family and Redistributed Connected Routes](#), on page 638. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol.
 - Step 4** Configure IP Pools with MPLS labels for input and output by applying the example configuration in [Configure IP Pools with MPLS Labels](#), on page 638.
 - Step 5** *Optional.* Bind DHCP service to work with MPLS labels for input and output in corporate networks by applying the example configuration in [Bind DHCP Service for Corporate Servers](#), on page 638.
 - Step 6** *Optional.* Bind AAA/RADIUS server group in corporate network to work with MPLS labels for input and output by applying the example configuration in [Bind AAA Group for Corporate Servers](#), on page 639.
 - Step 7** Save your configuration as described in the *System Administration Guide*.
-

Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second **ip vrf** command creates the route-distinguisher and route-target.

```
configure
context <context_name> -noconfirm
  ip vrf <vrf_name>
    router bgp <as_number>
      ip vrf <vrf_name>
        route-distinguisher {<as_value> | <ip_address>} <rt_value>
        route-target export {<as_value> | <ip_address>} <rt_value>
      end
```

Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

```
configure
context <context_name>
  router bgp <as_number>
    neighbor <ip_address> remote-as <AS_num>
    address-family vpnv4
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
    exit
  interface <bind_intf_name>
```

```
ip address <ip_addr_mask_combo>
end
```

Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```
configure
context <context_name>
router bgp <as_number>
address-family ipv4 <type> vrf <vrf_name>
redistribute connected
end
```

Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with MPLS labels for input and output.

```
configure
context <context_name> -noconfirm
ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name> mpls-label input <in_label_value>
output <out_label_value1> nexthop-forwarding-address <ip_addr_bgp_neighbor>
end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with MPLS labels for input and output in Corporate network.

```
configure
context <dest_ctxt_name>
interface <intfc_name> loopback
ip vrf forwarding <vrf_name>
ip address <bind_ip_address subnet_mask>
exit
dhcp-service <dhcp_svc_name>
dhcp ip vrf <vrf_name>
bind address <bind_ip_address> [ nexthop-forwarding-address <nexthop_ip_address> [
mpls-label input <in_mpls_label_value> output <out_mpls_label_value1> [ <out_mpls_label_value2>
]]]
dhcp server <ip_address>
end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <ip_address> **mpls-label input** <in_mpls_label_value> **output** <out_mpls_label_value1> applies DHCP over MPLS traffic.

Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with MPLS labels for input and output in Corporate network.

configure

```
context <dest_ctxt_name>
  aaa group <aaa_grp_name>
    radius ip vrf <vrf_name>
    radius attribute nas-ip-address address <nas_address> nexthop-forwarding-address
    <ip_address> mpls-label input <in_mpls_label_value> output < <out_mpls_label_value1>
    radius server <ip_address> encrypted key <encrypt_string> port <iport_num>
  end
```

Notes:

- *aaa_grp_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.
- Optional keyword **nexthop-forwarding-address** <ip_address> **mpls-label input** <in_mpls_label_value> **output** < <out_mpls_label_value1> associates AAA group for MPLS traffic.

Configuring BGP/MPLS VPN with Dynamic Labels

This section describes the procedures required to configure the system as an MPLS-CE to interact with a PE with dynamic MPLS label support.

The base configuration, as described in the *Routing* chapter in this guide, must be completed prior to attempt the configuration procedure described below.



Important

The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.



Important

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

To configure the system for BGP/MPLS VPN:

-
- | | |
|---------------|---|
| Step 1 | Create a VRF on the router and assign a VRF name by applying the example configuration in Create VRF with Route-distinguisher and Route-target , on page 640. |
| Step 2 | Set the neighbors and address family to exchange routing information and establish BGP peering with a peer router by applying the example configuration in Set Neighbors and Enable VPNv4 Route Exchange , on page 641. |
| Step 3 | Configure the address family and redistribute the connected routes domains into BGP by applying the example configuration in Configure Address Family and Redistributed Connected Routes , on page 641. This takes any routes from another protocol and redistributes them to BGP neighbors using the BGP protocol. |
| Step 4 | Configure IP Pools with dynamic MPLS labels by applying the example configuration in Configure IP Pools with MPLS Labels , on page 641. |
| Step 5 | <i>Optional.</i> Bind DHCP service to work with dynamic MPLS labels in corporate networks by applying the example configuration in Bind DHCP Service for Corporate Servers , on page 641. |
| Step 6 | <i>Optional.</i> Bind AAA/RADIUS server group in corporate network to work with dynamic MPLS labels by applying the example configuration in Bind AAA Group for Corporate Servers , on page 642. |
| Step 7 | <i>Optional.</i> Modify the configured IP VRF, which is configured to support basic MPLS functionality, for mapping between DSCP bit value and experimental (EXP) bit value in MPLS header for ingress and egress traffic by applying the example configuration in DSCP and EXP Bit Mapping , on page 642. |
| Step 8 | Save your configuration as described in the <i>System Administration Guide</i> . |
-

Create VRF with Route-distinguisher and Route-target

Use this example to first create a VRF on the router and assign a VRF name. The second **ip vrf** command creates the route-distinguisher and route-target.

```
configure
context <context_name> -noconfirm
  ip vrf <vrf_name>
  router bgp <as_number>
    ip vrf <vrf_name>
      route-distinguisher {<as_value> | <ip_address>} <rt_value>
      route-target export {<as_value> | <ip_address>} <rt_value>
      route-target import {<as_value> | <ip_address>} <rt_value>
    end
```

Notes:

- If export and import route targets are the same, alternate command **route-target both** {<as_value> | <ip_address>} <rt_value> can be used in place of **route-target import** and **route-target export** commands.

Set Neighbors and Enable VPNv4 Route Exchange

Use this example to set the neighbors and address family to exchange VPNv4 routing information with a peer router.

```
configure
context <context_name>
  mpls bgp forwarding
  router bgp <as_number>
    neighbor <ip_address> remote-as <AS_num>
    address-family vpnv4
    neighbor <ip_address> activate
    neighbor <ip_address> send-community both
  exit
interface <bind_intf_name>
  ip address <ip_addr_mask_combo>
end
```

Configure Address Family and Redistributed Connected Routes

Use this example to configure the **address-family** and to **redistribute** the connected routes or IP pools into BGP. This takes any routes from another protocol and redistributes them using the BGP protocol.

```
configure
context <context_name>
  router bgp <as_number>
    address-family ipv4 <type> vrf <vrf_name>
    redistribute connected
  end
```

Configure IP Pools with MPLS Labels

Use this example to configure IP Pools with dynamic MPLS labels.

```
configure
context <context_name> -noconfirm
  ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name>
end
```

Bind DHCP Service for Corporate Servers

Use this example to bind DHCP service with dynamic MPLS labels in Corporate network.

```
configure
context <dest_ctxt_name>
  interface <intfc_name> loopback
    ip vrf forwarding <vrf_name>
    ip address <bind_ip_address_subnet_mask>
  exit
  dhcp-service <dhcp_svc_name>
    dhcp ip vrf <vrf_name>
    bind address <bind_ip_address>
```

```

dhcp server <ip_address>
end

```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.

Bind AAA Group for Corporate Servers

Use this example to bind AAA server groups with dynamic MPLS labels in Corporate network.

```

configure
context <dest_ctxt_name>
  aaa group <aaa_grp_name>
  radius ip vrf <vrf_name>
  radius attribute nas-ip-address address <nas_address>
  radius server <ip_address> encrypted key <encrypt_string> port <iport_num>
end

```

Notes:

- *aaa_grp_name* is a pre-configured AAA server group configured in Context Configuration mode. Refer *AAA Interface Administration Reference* for more information on AAA group configuration.

DSCP and EXP Bit Mapping

Use this example to modify the configured IP VRF to support QoS mapping.

```

configure
context <context_name>
  ip vrf <vrf_name>
    mpls map-dscp-to-exp dscp <dscp_bit_value> exp <exp_bit_value>
    mpls map-exp-to-dscp exp <exp_bit_value> dscp <dscp_bit_value>
  end

```



Revised Marking for Subscriber Traffic

- [Revised Marking for Subscriber Traffic, page 643](#)

Revised Marking for Subscriber Traffic

Feature Description

802.1p/MPLS EXP marking helps in providing QoS treatment by prioritizing traffic at L2 level.

Currently, data traffic for different access types, such as GGSN, eHRPD, P-GW, and S-GW, refer to the QCI-QoS table and configure the appropriate 802.1p or MPLS-EXP (L2 QoS) markings based on the internal-qos value associated with particular row. However, the usage of internal-qos from the QCI-QoS table is not configurable and uses the default values. In addition, L2 QoS (802.1p/MPLS EXP) marking is not supported in GGSN, SAEGW, and GTPv1/eHRPD calls on P-GW.

With this feature, you can:

- Configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls.
- Mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. A new CLI command has been introduced to support service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Limitations

- This feature does not control the behavior of the control packets. The control packets (GTP-C) continue to get L2 marked based on DSCP derived L2 marking.
- This feature is not supported on standalone GGSN. It is supported on GnGp-GGSN node.

How It Works

You can configure internal priority in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. You can also mark subscriber traffic with either 802.1p or MPLS-EXP to enable or disable L2 marking. To

do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Behavior Changes for Different Services

This section describes behavior of this feature for different services. Please see the *Command Changes* section for more information on the CLI command options and its behavior:

GGSN/P-GW GTPv1 Calls:

Previous Behavior: Earlier, the traffic was not marked for data path. This was default behavior for GGSN.

New Behavior: A new CLI command has been introduced to mark the traffic based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked. When the feature is not enabled, traffic is not marked.

P-GW GTPv2, S-GW, SAEGW Calls:

Previous Behavior: StarOS release 16 onward, the QCI-QoS mapping feature used internal-QoS for L2 marking, which in turn uses QCI-Derived marking for data traffic. This was the default behavior for P-GW, S-GW, and SAEGW calls.

New Behavior: With this feature, the traffic is marked based on:

- QCI-Derived
- DSCP-Derived
- None

If the no or default option of the CLI command is used, then the traffic is not marked and the default behavior is executed. When the feature is not enabled, traffic is not marked.

Configuring Revised Marking for Subscriber Traffic

Earlier, the traffic was not marked for data path. This was default behavior for GGSN. Now, internal priority can be configured in QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls. Subscriber traffic can also be marked with either 802.1p or MPLS-EXP to enable or disable L2 marking. To do this, use the CLI command to configure service specific configuration to mark subscriber traffic. This L2 marking can be decided based on QCI and DSCP marking together or solely based on DSCP marking.

Configuring Internal Priority

To configure internal priority in the QCI-mapping table for the GGSN, GTPv1 P-GW, and SAEGW calls, use the following service specific configuration. This command in the GGSN service configuration overrides the behavior of QCI-QOS-mapping for data packets only.

```
configure
    context context_name
```



```

ggsn-service service_name
  internal-qos data { dscp-derived | none | qci-derived }
  { no | default } internal-qos data { dscp-derived | none | qci-derived }
end

```

Notes:

- **no:** Disables the specified functionality.
- **default:** Disables the functionality.
- **dscp-derived:** Data packets are marked at Layer 2 based on DSCP configured in qci-qos mapping table, then if DSCP is not configured in the qci-qos mapping table then data packets are not marked.
- **none:** Data packets are not marked with Layer 2 (MPLS EXP/802.1P) marking.
- **qci-derived:** Data packets are marked at Layer 2 based on internal-qos-priority configured in qci-qos mapping table. If internal-qos priority is not configured in the qci-qos mapping table, then the data packets are not marked.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show configuration**
- **show service-type { all | name service_name }**

Please see the *Monitoring and Troubleshooting Revised Marking for Subscriber Traffic* section for the command output.

Monitoring and Troubleshooting Revised Marking for Subscriber Traffic

The following section describes commands available to monitor Revised Marking for Subscriber Traffic.

Internal Priority Show Commands

The following section describes commands available to monitor Internal Priority.

show configuration

This command displays the following output:

- When **internal-qos data** is configured as **none**:
internal-qos data none
- When **internal-qos data** is configured as **qci-derived**:
internal-qos data qci-derived
- When **internal-qos data** is configured as **dscp-derived**:
internal-qos data dscp-ds-derived
- When **internal-qos data** is **not configured**:
no internal-qos data

show service-type { all | name service_name }

This command displays the following output:

- When **internal-qos data** is configured as **none**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:        None
```

- When **internal-qos data** is configured as **qci-derived**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:        QCI Derived
```

- When **internal-qos data** is configured as **dscp-derived**:

```
Internal QOS Application:    Enabled
Internal QoS Policy:        DSCP Derived
```

- When **internal-qos data** is **not configured**:

```
Internal QOS Application:    Backward-compatible
```



CHAPTER 31

Rejection/Redirection of HA Sessions on Network Failures

This chapter provides information on configuring an enhanced, or extended, service. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

This chapter contains the following topics:

- [Overview, page 647](#)
- [Configuring HA Session Redirection, page 648](#)
- [RADIUS Attributes, page 651](#)

Overview

This feature enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner.

The way this is implemented in the system is as follows:

- A policy is configured in the HA service that tells the service what action to take when network connectivity is lost. New calls are either directed to one of up to 16 different IP addresses or all new calls are rejected until network connectivity is restored.
- In the destination context, a network reachability server is configured. This is a device on the destination network to which ping packets are periodically sent to determine if the network is reachable. As soon as a network reachability server is configured, pinging of the server commences whether or not the server name is bound to a subscriber or an IP pool.
- The name of the network reachability server configured in the destination context is bound to either a local subscriber profile or an IP pool. If the subscriber is authenticated by an AAA server, RADIUS attributes may specify the network reachability server for the subscriber. (If an IP pool has a network reachability server name bound to it, that takes precedence over both the RADIUS attributes and the local subscriber configuration.)

Configuring HA Session Redirection

This section provides instructions for configuring rejection or redirection of HA sessions on the event of a network failure. These instructions assume that there is a destination context, and HA service, an IP pool, and a subscriber already configured and that you are at the root prompt for the Exec mode:

```
[local]host_name
```

Step 1 Enter the global configuration mode by entering the following command:

configure

The following prompt appears:

```
[local]host_name(config)
```

Step 2 Enter context configuration mode by entering the following command:

context <context_name>

context_name is the name of the destination context where the HA service is configured. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ctx)
```

Step 3 Enter the HA service configuration mode by entering the following command:

ha-service <ha_service_name>

ha_service_name is the name of the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ha-service)
```

Step 4 Configure the action for the HA service to take when network connectivity is lost by entering the following command:

```
policy nw-reachability-fail { reject [ use-reject-code { admin-prohibited | insufficient-resources } ] | redirect
<ip_addr1> [ weight <value> ] [ <ip_addr2> [ weight <value> ] ] ... [ <ip_addr16> [ weight <value> ] ]
}
```

Keyword/Variable	Description
reject	Upon network reachability failure reject all new calls for this context.
use-reject-code { admin-prohibited insufficient-resources }	When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.
redirect <ip_addr1> [weight <value>] [<ip_addr2> [weight <value>]] ... [<ip_addr16> [weight <value>]]	<p>Upon network reachability failure redirect all calls to the specified IP address.</p> <p><ip_addr>: This must be an IPv4 address. Up to 16 IP addresses and optional weight values can be entered on one command line.</p> <p>weight <value>: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified, the entry is automatically assigned a weight of 1. <value> must be an integer from 1 through 10.</p>

Step 5 Enter the following command to return to the context configuration mode:

exit

The following prompt appears:

[<context_name>]host_name(config-ctx)

Step 6 Specify the network device on the destination network to which ping packets should be sent to test for network reachability, by entering the following command:

nw-reachability server <server_name> [**interval** <seconds>] [**local-addr** <ip_addr>] [**num-retry** <num>] [**remote-addr** <ip_addr>] [**timeout** <seconds>]

Keyword/Variable	Description
<i>server_name</i>	A name for the network device that is sent ping packets to test for network reachability.
interval <seconds>	Default: 60 seconds Specifies the frequency in seconds for sending ping requests.<seconds> must be an integer from 1 through 3600.
local-addr <ip_addr>	Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. <ip_addr> must be an IP v4 address.
num-retry <num>	Default: 5 Specifies the number of retries before deciding that there is a network-failure. <num> must be an integer from 0 through 100.
remote-addr <ip_addr>	Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. <ip_addr> must be an IPv4 address.
timeout <seconds>	Default: 3 seconds Specifies how long to wait, in seconds, before retransmitting a ping request to the remote address. <seconds> must be an integer from 1 through 10.

- Step 7** Repeat *step 6* to configure additional network reachability servers.
- Step 8** To bind a network reachability server to an IP pool, continue with *step 9*. To bind a network reachability server to a local subscriber profile, skip to *step 11*.

- Step 9** To bind a network reachability server name to an IP pool, enter the following command:

ip pool *<pool_name>* **nw-reachability server** *<server_name>*

<i><pool_name></i>	The name of an existing IP pool in the current context.
nw-reachability server <i><server_name></i>	Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration or RADIUS attribute. <i><server_name></i> : The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.

- Step 10** Repeat *step 9* for additional IP pools in the current context then skip to *step 13*.

- Step 11** Enter the subscriber configuration mode by entering the following command:

subscriber { **default** | **name** *<subs_name>* }

Where **default** is the default subscriber for the current context and *subs_name* is the name of the subscriber profile that you want to configure for network reachability. The following prompt appears:

[*<context_name>*] *host_name*(**config-subscriber**)

- Step 12** To bind a network reachability server name to the current subscriber in the current context, enter the following command:

nw-reachability server *<server_name>*

Where *server_name* is the name of a network reachability server that has been defined in the current context.

- Step 13** Return to the executive mode by entering the following command:

end

The following prompt appears:

[*local*] *host_name*

- Step 14** Enter the executive mode for the destination context for which you configured network reachability by entering the following command:

context *<context_name>*

Where *context_name* is the name of the destination context for which you configured network reachability. The following prompt appears:

[*context_name*] *host_name*

- Step 15** Check the network reachability server configuration by entering the following command

show nw-reachability server all

The output of this command appears similar to the following:

```

Server          remote-addr    local-addr    state
-----
nw-server1      192.168.100.20 192.168.1.10  Down
Total Network Reachability Servers: 1 Up: 0

```

Ensure that the remote and local addresses are correct. The state column indicates whether or not the server is reachable (Up) or unreachable (Down).

- Step 16** Check the HA service policy by entering the following command:

show ha-service name *<ha_service_name>*

Where *<ha_service_name>* is the name of the HA service in the current context for which you configured a network reachability policy. The output of this command includes information about the network reachability policy that looks similar to the following:

```
NW-Reachability Policy: Reject      (Reject code: Admin Prohibited)
```

Step 17 Check the network reachability server name bound to an IP pool by entering the following command:

show ip pool pool-name *<pool_name>*

Where *<pool_name>* is the name of the IP pool to which you bound a network reachability server name. The output of this command includes information about the network reachability server name that looks similar to the following:

```
Network Reachability Detection Server: nw-server1
```

Step 18 Check the network reachability server name bound to a local subscriber profile by entering the following command:

show subscribers configuration username *<subscriber_name>*

Where *<subscriber_name>* is the name of the local subscriber to which you bound a network reachability server name. The output of this command includes information about the network reachability server name that looks similar to the following:

```
network reachability detection server name: nw-server1
```

Step 19 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

RADIUS Attributes

Attributes defined in a subscriber profile stored remotely on a RADIUS server can be used to bind the network reachability server to a subscriber session. Use the following attributes to bind a network reachability server to a subscriber session;

- SN-Nw-Reachability-Server-Name
- SN1-Nw-Reachability-Server-Name

The attributes have one possible value, which is a variable that is a string of from 1 to 15 characters in length. This should be the name of the configured network reachability server.

The **SN-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent
- starent-835

The **SN1-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent-vsai
- starent-vsai-835

Refer to the *AAA Interface Administration and Reference* for more details.



Policy Forwarding

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model before using the procedures in this chapter.

Sections in this chapter include:

- [Overview, page 653](#)
- [IP Pool-based Next Hop Forwarding, page 654](#)
- [Subscriber-based Next Hop Forwarding, page 654](#)
- [ACL-based Policy Forwarding, page 655](#)

Overview

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.

IP Pool-based Next Hop Forwarding

When an IP pool in a destination context has a Next Hop Forwarding address specified, any subscriber that obtains an IP address from that IP pool has all data coming from the mobile node automatically forwarded to the specified Next Hop Forwarding address.

For more information on creating IP pools, refer to the *System Administration Guide* and for additional information on the **ip pool** command, refer to the *Command Line Interface Reference*.

Configuring IP Pool-based Next Hop Forwarding

Configure Next Hop Forwarding on an existing IP Pool in a destination context by applying the following example configuration:

```
configure
  context <context_name>
    ip pool <pool_name> nexthop-forwarding-address <forwarding_ip_address>
  end
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Subscriber-based Next Hop Forwarding

When a subscriber configuration has a Next Hop Forwarding address specified, any sessions authenticated as that subscriber have all data coming from the mobile node automatically forwarded to the specified Next Hop Forwarding address.

Configuring Subscriber-based Next Hop Forwarding

Configure Next Hop Forwarding for a specific subscriber by applying the following example configuration:

```
configure
  context <context_name>
    subscriber name <subs_name>
      nexthop-forwarding-address <forwarding_ip_address>
    end
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

ACL-based Policy Forwarding

ACL-based Policy Forwarding is a feature in the system that forwards subscriber data based on policies defined in Access Control Lists (ACLs). When ACLs are applied to access groups, priorities are given to the ACLs. The ACL applied with the highest priority is used to define the policy that is used for forwarding the subscriber data.



Important

Refer to *Access Control Lists* for additional information on creating and using ACLs.

Configuring ACL-based Policy Forwarding

Configure ACL-based Policy Forwarding by applying the following example configuration:

```
configure
  context <context_name>
    ip access-list <acl_name>
      redirect <interface_name> <next_hop_address> <criteria>
    exit
```

The following example specifies that any IP packet coming from any system on the 192.168.55.0 network that has a destination host address of 192.168.80.1 is to be redirected, or forwarded, through the system interface named *interface2* to the host at 192.168.23.12:

```
redirect interface2 192.168.23.12 ip 192.168.55.0 255.255.255.0 host 192.168.80.1
```

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Applying the ACL to an IP Access Group

To apply the ACL to the IP access group for the current destination context, go to *Applying the ACL to a Destination Context*.

To apply the ACL to the IP access group for an interface in the current destination context, go to [Applying the ACL to an Interface in a Destination Context](#), on page 656.

Applying the ACL to a Destination Context

Step 1

At the context configuration mode prompt, enter the following command:

```
ip access-group <acl_name> { in | out } <priority-value>
```

Step 2

Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Applying the ACL to an Interface in a Destination Context

-
- Step 1** Set parameters for inbound data by applying the following example configuration:
- ```
configure
 context <context_name>
 interface <interface_name>
 ip access-group <acl_name> in <priority-value>
 end
```
- Step 2** Set parameters for outbound data by applying the following example configuration:
- ```
configure
  context <context_name>
    interface <interface_name>
      ip access-group <acl_name> out <priority-value>
    end
```
- Step 3** Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
-



Proxy-Mobile IP

This chapter describes system support for Proxy Mobile IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model before using the procedures in this chapter.

Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:

- [Overview, page 657](#)
- [How Proxy Mobile IP Works in 3GPP2 Network, page 660](#)
- [How Proxy Mobile IP Works in 3GPP Network, page 666](#)
- [How Proxy Mobile IP Works in WiMAX Network, page 670](#)
- [How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication, page 675](#)
- [Configuring Proxy Mobile-IP Support, page 680](#)

Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.



Important

Proxy Mobile IP is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Table 44: Applicable Products and Relevant Sections

Applicable Product(s)	Refer to Sections
PDSN	<ul style="list-style-type: none"> • Proxy Mobile IP in 3GPP2 Service, on page 659 • How Proxy Mobile IP Works in 3GPP2 Network, on page 660 • Configuring FA Services, on page 680 • Configuring Proxy MIP HA Failover, on page 682 • <i>Configuring HA Services</i> • Configuring Subscriber Profile RADIUS Attributes, on page 682 • RADIUS Attributes Required for Proxy Mobile IP, on page 683 • Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN, on page 684 • Configuring Default Subscriber Parameters in Home Agent Context, on page 685
GGSN	<ul style="list-style-type: none"> • Proxy Mobile IP in 3GPP Service, on page 659 • How Proxy Mobile IP Works in 3GPP Network, on page 666 • Configuring FA Services, on page 680 • Configuring Proxy MIP HA Failover, on page 682 • <i>Configuring HA Services</i> • Configuring Subscriber Profile RADIUS Attributes, on page 682 • RADIUS Attributes Required for Proxy Mobile IP, on page 683 • Configuring Default Subscriber Parameters in Home Agent Context, on page 685 • Configuring APN Parameters, on page 685
ASN GW	<ul style="list-style-type: none"> • Proxy Mobile IP in WiMAX Service, on page 660 • How Proxy Mobile IP Works in WiMAX Network, on page 670 • Configuring FA Services, on page 680 • Configuring Proxy MIP HA Failover, on page 682 • <i>Configuring HA Services</i> • Configuring Subscriber Profile RADIUS Attributes, on page 682 • RADIUS Attributes Required for Proxy Mobile IP, on page 683 • Configuring Default Subscriber Parameters in Home Agent Context, on page 685

Applicable Product(s)	Refer to Sections
PDIF	<ul style="list-style-type: none"> • How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication, on page 675 • Configuring FA Services, on page 680 • Configuring Proxy MIP HA Failover, on page 682 • Configuring HA Services • Configuring Subscriber Profile RADIUS Attributes, on page 682 • RADIUS Attributes Required for Proxy Mobile IP, on page 683 • Configuring Default Subscriber Parameters in Home Agent Context, on page 685

Proxy Mobile IP in 3GPP2 Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

How Proxy Mobile IP Works in 3GPP2 Network

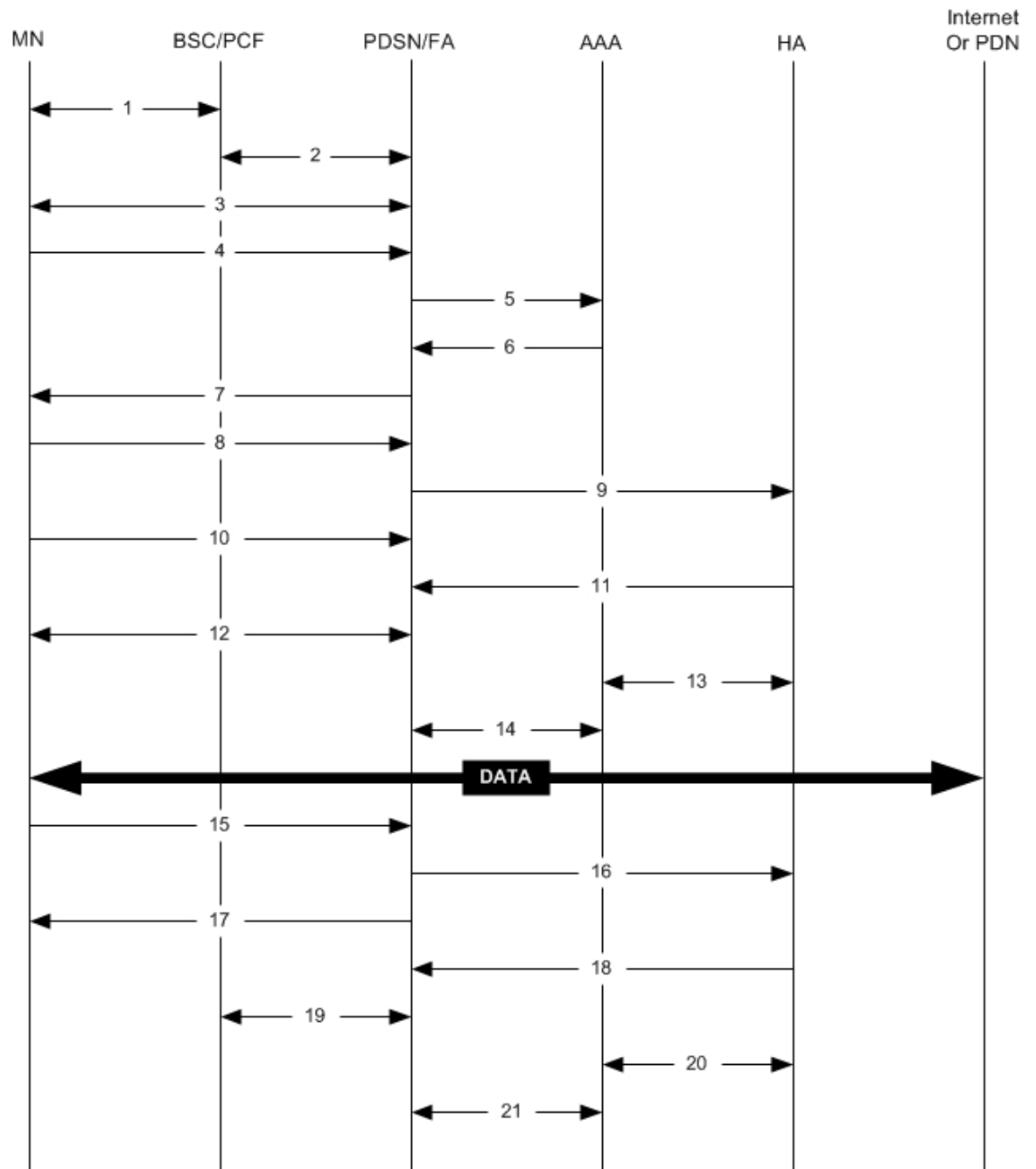
This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 88: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow



335164

Table 45: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

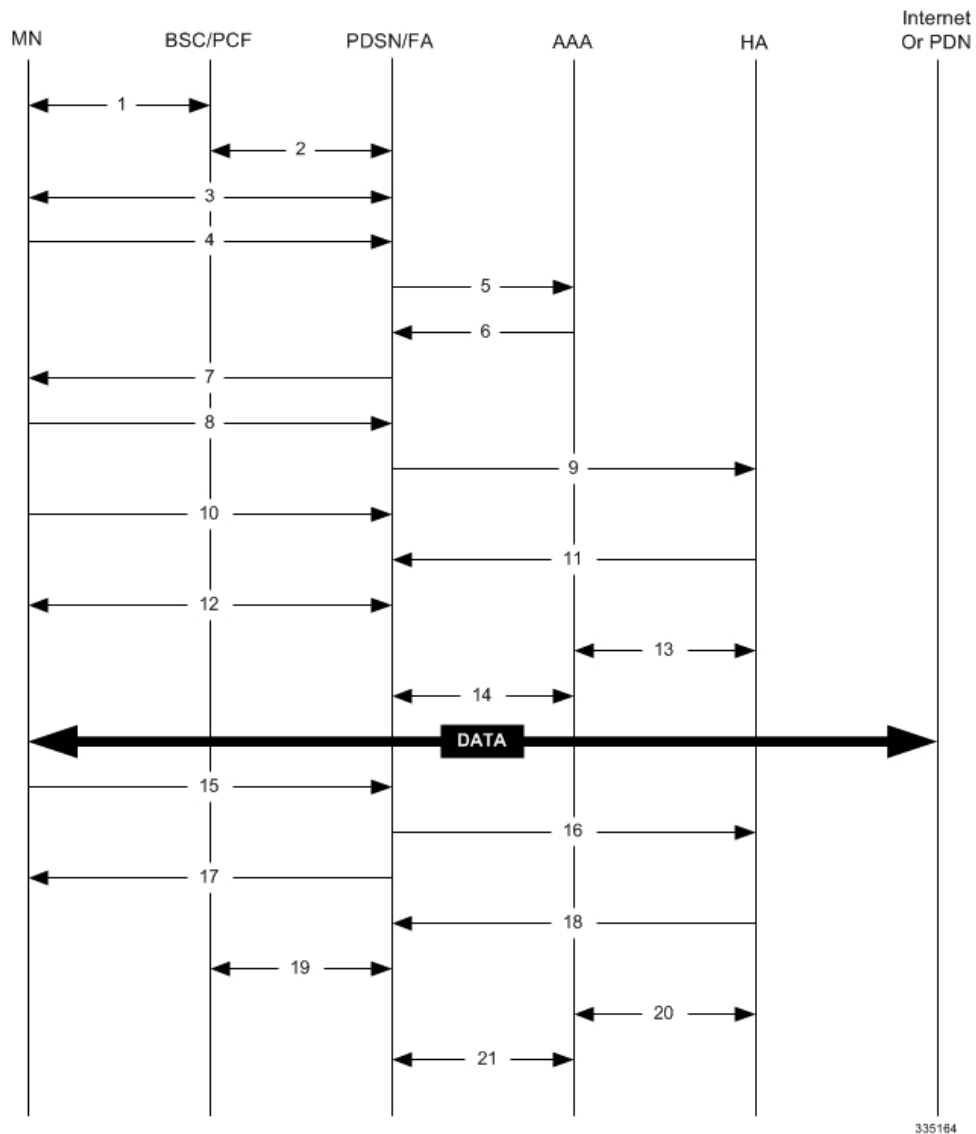
Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against its pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.

Step	Description
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 89: HA Assigned IP Address Proxy Mobile IP Call Flow



335164

Table 46: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.

Step	Description
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN/FA to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface

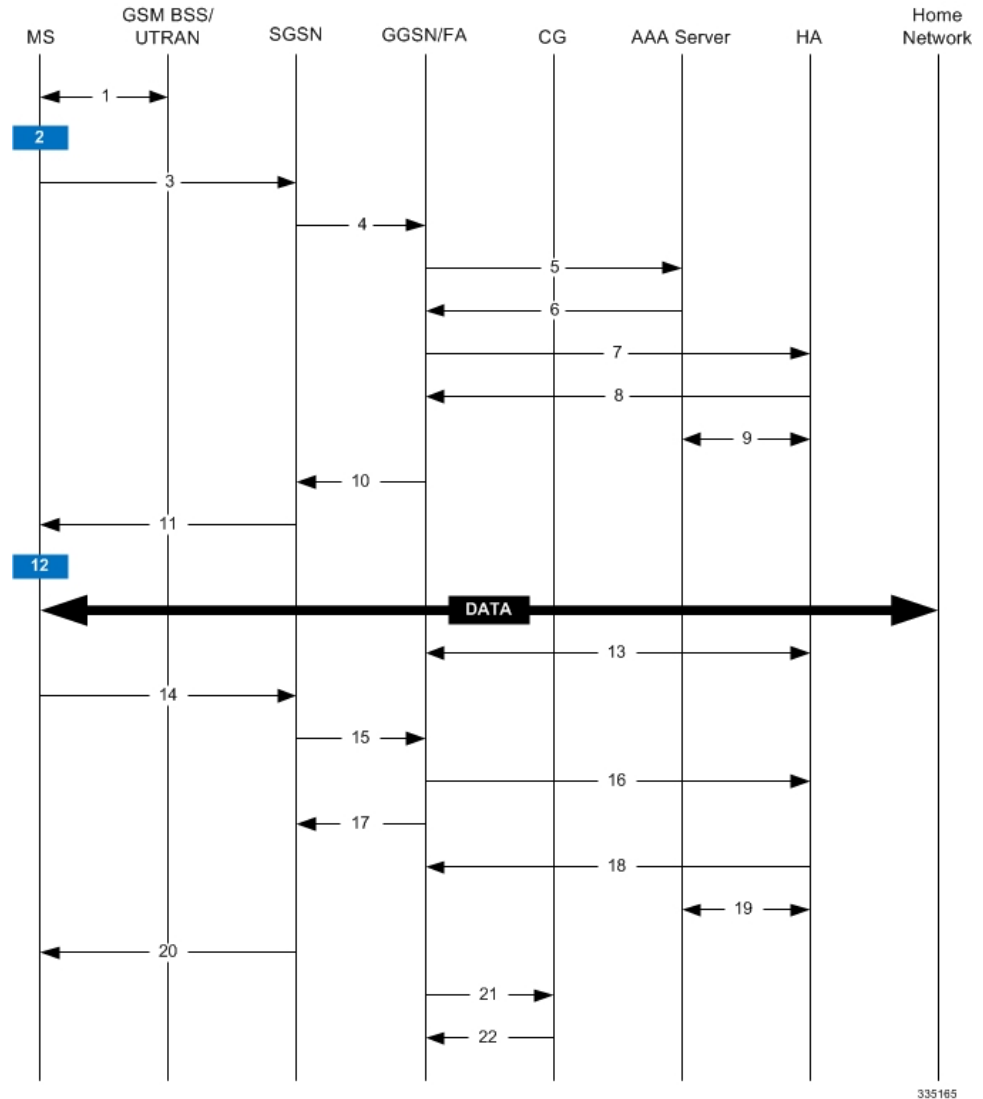
Step	Description
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network.

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in 3GPP service.

Figure 90: Proxy Mobile IP Call Flow in 3GPP



335165

Table 47: Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

Step	Description
2	<p>The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the MS to place it into PPP mode.</p> <p>The Link Control Protocol (LCP) is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.</p> <p>Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.</p>
3	<p>The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.</p>
4	<p>The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signalling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).</p>
5	<p>The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.</p> <p>From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.</p> <p>Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings.</p> <p>If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to a AAA server.</p>
6	<p>If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.</p>
7	<p>If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).</p>
8	<p>The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.</p>

Step	Description
9	The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10	The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
11	The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
12	The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
13	The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
14	The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
15	The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16	The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
17	The GGSN returns a Delete PDP Context Response message to the SGSN.
18	The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19	The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20	The SGSN returns a Deactivate PDP Context Accept message to the MS.
21	The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
22	For each accounting message received from the GGSN, the CG responds with an acknowledgement.

How Proxy Mobile IP Works in WiMAX Network

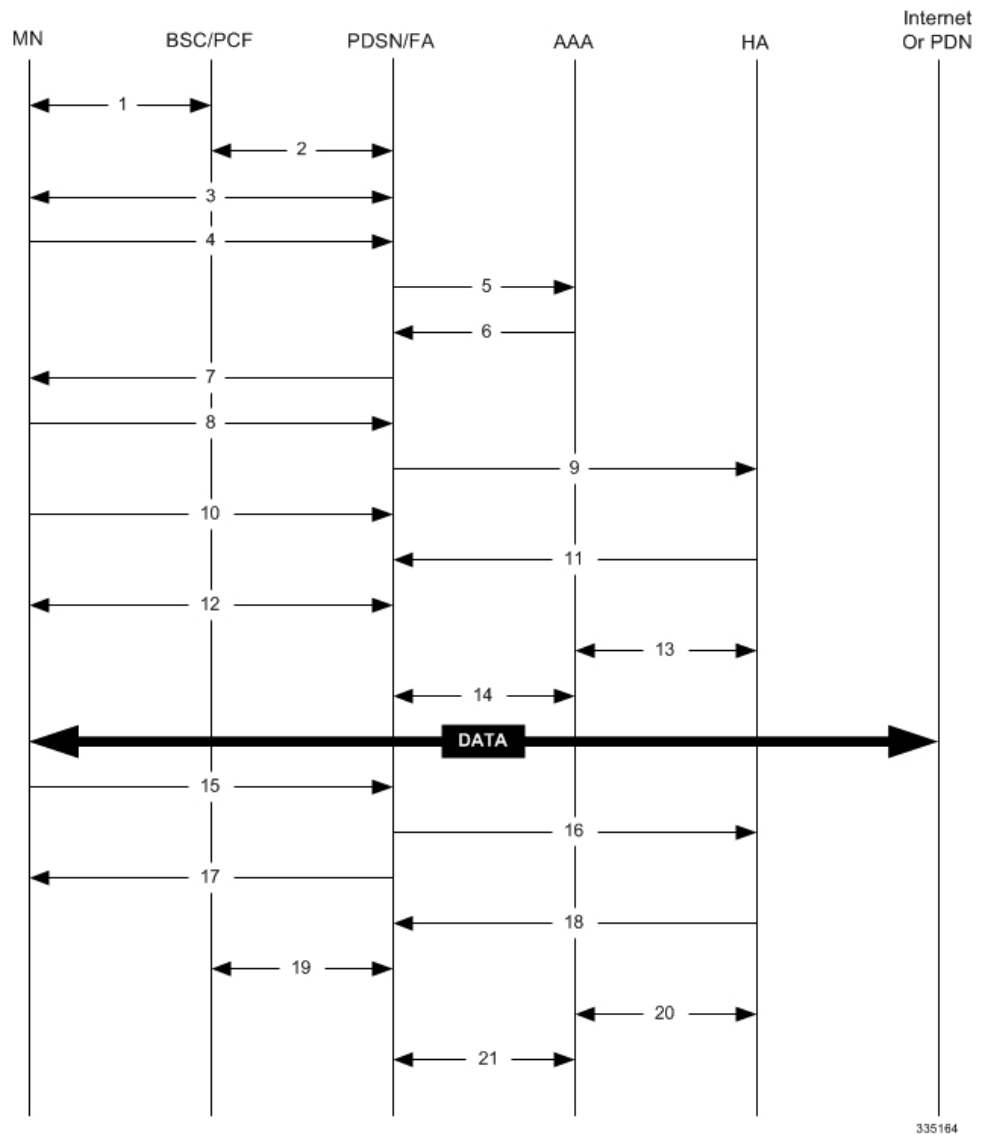
This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and ASN GW/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.

Figure 91: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow



335164

Table 48: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.

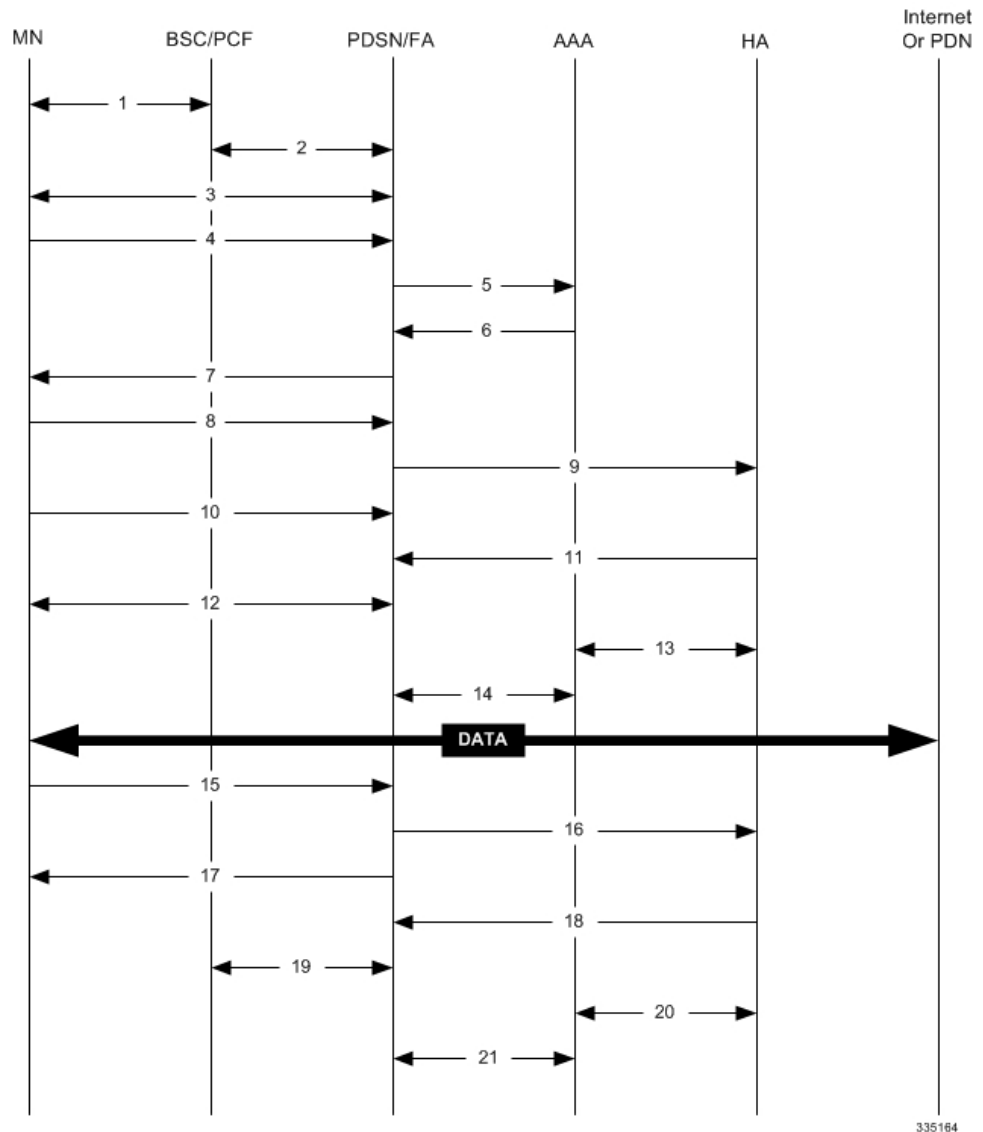
Step	Description
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The ASN GW/FA sends a EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against its pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.

Step	Description
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 92: HA Assigned IP Address Proxy Mobile IP Call Flow



335164

Table 49: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The ASN GW/FA sends an EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.
16	The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.

Step	Description
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers. Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool. The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.

Figure 93: Proxy-MIP Call Setup using CHAP Authentication

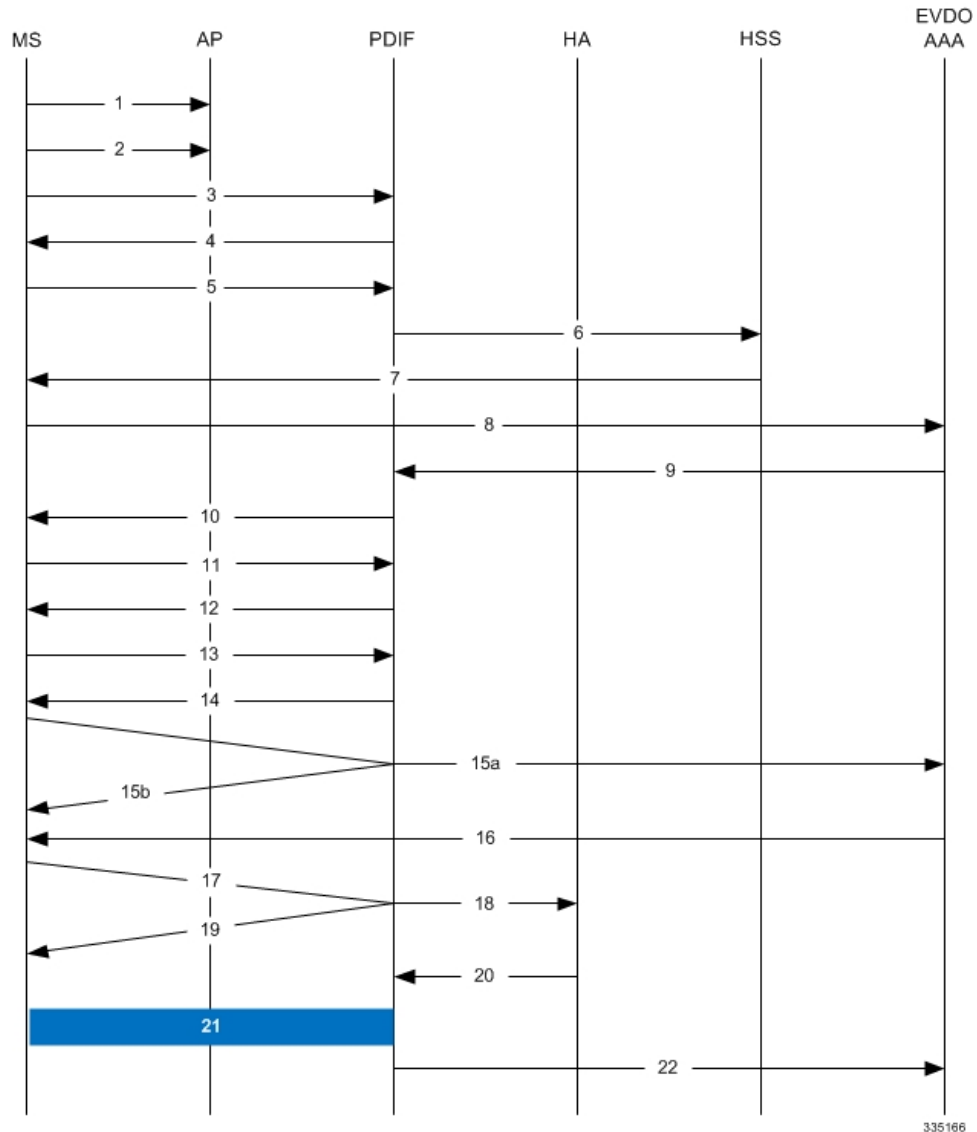


Table 50: Proxy-MIP Call Setup using CHAP Authentication

Step	Description
1	On connecting to WiFi network, MS first send DNS query to get PDIF IP address
2	MS receives PDIF address from DNS

Step	Description
3	MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.
4	PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP address in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDIF service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Response. PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.
5	On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload which contains the NAI, SA, TSr, CP (requesting IP address and DNS address) payloads. MS will not include AUTH payload to indicate that it will use EAP methods.
6	On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA servers are selected based on domain profile, default subscriber template or default domain configurations. PDIF includes Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details are explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Request from MS.
7	PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Payload AVP contents and sends IKE_AUTH Response back to MS in the EAP payload. PDIF allows IDr and CERT configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is configured to do so.
8	MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AUTH Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challenge received from MS.
9	The AAA server sends the DEA back to the PDIF with Result-Code AVP as "success." The EAP-Payload AVP message also contains the EAP result code with "success." The DEA also contains the IMSI for the user, which is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions such as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.
10	PDIF sends the IKE_AUTH Response back to MS with the EAP payload.
11	MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed from the keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS Notify payload also.

Step	Description
12	<p>PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH payload computed from the MSK. PDIF does not assign any IP address for the MS pending second authentication. Nor will the PDIF include any configuration payloads.</p> <p>a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify payload is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 session by sending INFORMATIONAL (Delete) Request. b. If ANOTHER_AUTH_FOLLOWS Notify payload is not present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. However, if proxy-mip-required is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ. When PDIF receives the Proxy-MIP RRP, it takes the Home Address (and DNS addresses if any) and sends the IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. In either case, IKEv2 setup will finish at this stage and IPsec tunnel gets established with a Tunnel Inner Address (TIA).</p>
13	<p>MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include the NAI. This NAI may be completely different from the NAI used in the first authentication.</p>
14	<p>On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second authentication methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP methods may be either EAP-Passthru or EAP-Terminated.</p> <p>a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload including challenge. b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC. c. MS processes the IKE_AUTH Response:</p> <ul style="list-style-type: none"> • If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the challenge, compute the response and send IKE_AUTH Request with EAP payload including Challenge and Response. • If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the MS sends legacy-Nak with EAP-GTC.
15(a)	<p>PDIF receives the new IKE_AUTH Request from MS.</p> <p>If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Access Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.).</p>
15(b)	<p>If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_AUTH Response with EAP-GTC.</p>
16	<p>PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.</p>
17	<p>PDIF receives the final IKE_AUTH Request with AUTH payload.</p>
18	<p>PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Agent if proxy-mip-required is enabled. The HA address may be received from the RADIUS server in the Access Accept (Step 16) or may be locally configured. PDIF may also remember the HA address from the first authentication received in the final DEA message.</p>

Step	Description
19	If proxy-mip-required is disabled, PDIF assigns the IP address from the local pool.
20	PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.
21	PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also sets up the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by including the CP payload with the IP address and optionally the DNS addresses. This completes the setup.
22	PDIF sends a RADIUS Accounting start message.

**Important**

For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.

Figure 94: Proxy-MIP Call Setup using PAP Authentication

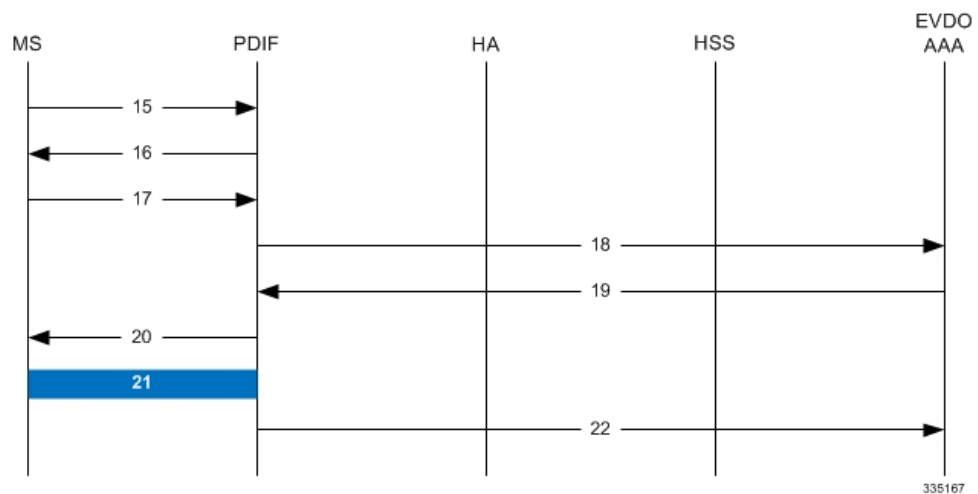


Table 51: Proxy-MIP Call Setup using PAP Authentication

Step	Description
15	MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.
16	PDIF then initiates EAP-GTC procedure, and requests a password from MS.
17	MS includes an authentication password in the EAP payload to PDIF.

Step	Description
18	Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Name attribute and PAP-password.
19	Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may include Framed-IP-Address attribute.
20	The attribute content in the Access Accept message is encoded as EAP payload with EAP success when PDIF sends the IKE_AUTH Response to the MS.
21	The MS and PDIF now have a secure IPSec tunnel for communication.
22	Pdif sends an Accounting START message.

Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:



Important

Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.



Important

These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

```
configure
context <context_name>
fa-service <fa_service_name>
```

```

proxy-mip allow
proxy-mip max-retransmissions <integer>
proxy-mip retransmission-timeout <seconds>
proxy-mip renew-percent-time percentage
fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number { encrypted
secret enc_secret | secret secret } [ description string ] [ hash-algorithm { hmac-md5 | md5 |
rfc2002-md5 } | replay-protection { timestamp | nonce } | timestamp-tolerance tolerance ]
authentication mn-ha allow-noauth
end

```

Notes:

- The **proxy-mip max-retransmissions** command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- **proxy-mip retransmission-timeout** configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
- **proxy-mip renew-percent-time** configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of **600** seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after **300** seconds have passed.

- Use the **fa-ha-spi remote-address** command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the *Command Line Interface Reference* for the full command syntax.



Important

Note that FA-HA SPIs **must** be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the **authentication mn-ha allow-noauth** command to configure the FA service to allow communications from the HA without authenticating the HA.

Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Proceed to the optional [Configuring Proxy MIP HA Failover, on page 682](#) to configure Proxy MIP HA Failover support or skip to the *Configuring HA Services* to configure HA service support for Proxy Mobile IP.

Configuring Proxy MIP HA Failover

Use this example to configure Proxy Mobile IP HA Failover:



Important

This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:

configure

context <context_name>

fa-service <fa_service_name>

proxy-mip ha-failover [**max-attempts** <max_attempts> | **num-attempts-before-switching** <num_attempts> | **timeout** <seconds>]

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.



Important

Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.



Important

Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

Table 52: Required RADIUS Attributes for Proxy Mobile IP

Attribute	Description	Values
SN-Subscriber-Permission OR SN1-Subscriber-Permission	Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute must be set to Simple IP.	<ul style="list-style-type: none"> • None (0) • Simple IP (0x01) • Mobile IP (0x02) • Home Agent Terminated Mobile IP (0x04)
SN-Proxy-MIP OR SN1-Proxy-MIP	Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute must be enabled to support Proxy Mobile IP.	<ul style="list-style-type: none"> • Disabled - do not perform compulsory Proxy-MIP (0) • Enabled - perform compulsory Proxy-MIP (1)
SN-Simultaneous-SIP-MIP OR SN1-Simultaneous-SIP-MIP	Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services. Note Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will not allow simultaneous Simple IP and Mobile IP sessions for the MN.	<ul style="list-style-type: none"> • Disabled (0) • Enabled (1)
SN-PDSN-Handoff-Req-IP-Addr OR SN1-PDSN-Handoff-Req-IP-Addr	Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.	<ul style="list-style-type: none"> • Disabled - do not reject (0) • Enabled - reject (1)

Attribute	Description	Values
3GPP2-MIP-HA-Address	This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.	IPv4 Address

Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

configure

context <context_name>

subscriber name <subscriber_name>

permission pdsn-simple-ip

proxy-mip allow

inter-psdn-handoff require ip-address

mobile-ip home-agent <ha_address>

<optional> **mobile-ip home-agent** <ha_address> **alternate**

ip context-name <context_name>

end

Verify that your settings for the subscriber(s) just configured are correct.

show subscribers configuration username <subscriber_name>

Notes:

- Configure the system to enforce the MN's use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the **inter-psdn-handoff require ip-address** command.
- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the **mobile-ip home-agent ha_address alternate** command to specify the secondary, or alternate HA.
- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

configure

context <context-name>


```
subscriber name <subscriber_name>
proxy-mip require
```

Note

subscriber_name is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

```
configure
context <context_name>
ip context-name <context_name>
end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.



Important

This is an optional configuration. In addition, attributes returned from the subscriber's profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name
```

Step 1

Enter the configuration mode by entering the following command:

```
configure
```

The following prompt appears:

```
[local]host_name(config)
```

Step 2

Enter context configuration mode by entering the following command:

```
context <context_name>
```

context_name is the name of the system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive. The following prompt appears:

```
[<context_name>]host_name(config-ctx)
```

Step 3

Enter the configuration mode for the desired APN by entering the following command:

```
apn <apn_name>
```

apn_name is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). The following prompt appears:

```
[<context_name>]host_name(config-apn)
```

Step 4

Enable proxy Mobile IP for the APN by entering the following command:

```
proxy-mip required
```

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

Step 5 *Optional.* GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:
proxy-mip null-username static-homeaddr

This command will enables the accepting of MIP Registration Request without NAI extensions in this APN.

Step 6 Return to the root prompt by entering the following command:
end

The following prompt appears:

[local]host_name

Step 7 Repeat *step 1* through *step 6* as needed to configure additional APNs.

Step 8 Verify that your APNs were configured properly by entering the following command:

show apn { all | name <apn_name> }

The output is a detailed listing of configured APN parameter settings.

Step 9 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



QoS Management

This segment describes the Quality of Service (QoS) management on Cisco® ASR 5500 chassis and explains how it is configured.

The product Administration Guides provide examples and procedures for configuration of basic services on the system. You should select the configuration example that best meets your service model and configure the required elements for that model as described in the respective product Administration Guide, before using the procedures described below.

- [Introduction, page 687](#)
- [Dynamic QoS Renegotiation, page 687](#)
- [Network Controlled QoS \(NCQoS\), page 690](#)
- [Configuring Dynamic QoS Renegotiation, page 691](#)
- [Configuring Network Controlled QoS \(NCQoS\), page 694](#)
- [Monitoring Dynamic QoS Renegotiation Operation, page 695](#)

Introduction

The QoS Traffic Policing functionality supported by the GGSN implements QoS for subscribers based on the configuration of the APN template. As a result, all subscriber PDP contexts using the APN receive the same QoS level. This could lead to unused or under-utilized bandwidth by some subscribers thus reducing the amount of resources available to others.

Dynamic QoS Renegotiation

Dynamic QoS Renegotiation minimizes the risk of bandwidth mis-appropriation. This feature allows the GGSN to analyze application traffic, and trigger QoS renegotiation with the SGSN to optimize service performance.

In Dynamic QoS Renegotiation, the GGSN performs packet inspection of application traffic to detect the type of service being utilized and automatically renegotiates the QoS to the appropriate level with a maximum QoS level corresponding to the level granted by the HLR.

QoS renegotiation is performed by sending an Update PDP Context Request to the SGSN. This solution is optimal since the appropriate QoS level is always granted to the subscriber without any requirement on the handset or on the core network. The only prerequisite is QoS renegotiation support on the SGSN. In this model, over reservation of radio resources is avoided, while maintaining the appropriate bandwidth for subscribers with real requirements.

The ASR 5500 supports L7 stateful analysis and QoS Renegotiation. These functions combine to become Dynamic QoS Renegotiation. The system also generates CDRs (or real time charging information) that includes the current QoS information and the service accessed. This enables intelligent application-based charging of services, taking into account the granted QoS. It also enables rebates when it was not possible to provide the QoS level required by an application.

**Important**

For L7 traffic analysis an ECSv2 license is required.

How Dynamic QoS Renegotiation Works

Implementation of Dynamic QoS Renegotiation involves the following:

- Initial QoS
- Service Detection
- Classification of Application Traffic
- Quality of Service Renegotiation

Initial QoS

When the session is established, an initial level of QoS must be assigned to the subscriber. The GGSN may either grant the requested QoS, or grant a lower QoS level (minimum or intermediate level). The initial QoS remains in effect until the SGSN or GGSN requests a change. When Dynamic QoS Renegotiation is enabled, there are several conditions when the system would request a QoS change.

- Services detected that do not need high QoS: After a configurable time period of a subscriber having terminated services that require high QoS, the system could lower the QoS to a value more appropriate to the services actually being used.
- Services detected that require higher QoS: As soon as a subscriber begins using a service that needs a high QoS, the system immediately attempts to raise the QoS through its service detection capability.

Service Detection

The Application analysis approach to service detection uses application level (L7) information. In the ASR 5500 chassis, application analysis is stateful—keeping track of the application state.

**Important**

For L7 traffic analysis ECSv2 license is required.

Classification of Application Traffic

Application traffic can be classified into the following: Conversational, Streaming, Interactive 1, Interactive 2, Interactive 3, or Background. Traffic class can be configured in the charging-action, but it does not take direction as a parameter. However, you can configure a rule matching uplink-only or downlink-only packets and associate it with the charging-action.

QoS renegotiation requires knowing what kind of data packets are flowing through for a particular user to associate a given traffic class with the user's current usage pattern. This is done through packet inspection for a subscriber profile via an Access Control List (ACL). Limits for each traffic class can be configured in the APN. The same infrastructure is reused to perform Dynamic QoS Renegotiation.

After classification of traffic and if required by subscriber profile, Dynamic QoS Renegotiation takes place.

L4 Packet Inspection

L4 packet analysis has no or low impact on the system performance with very limited impact on system capacity. L4 packet inspection is fully supported by the system.

L7 Packet Inspection

L7 packet analysis has a greater impact on system performance with very limited impact on the system capacity. L7 packet inspection involves complete application layer analysis and copes with customized applications.

QoS Renegotiation for a Subscriber QoS Profile

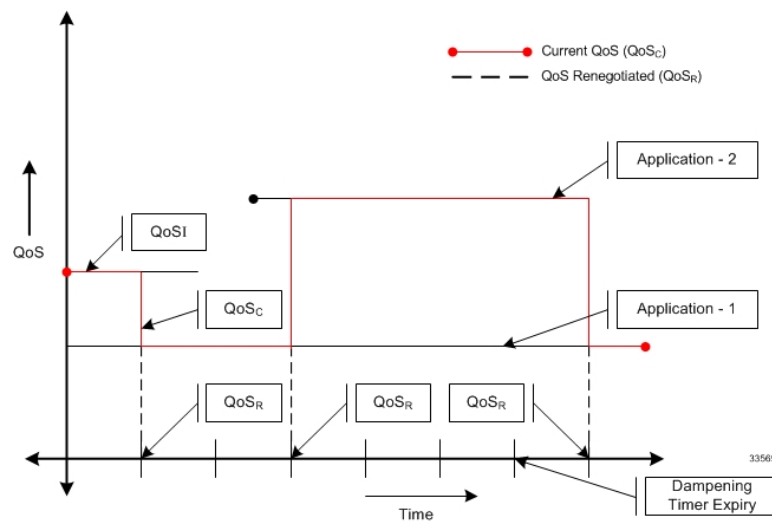
The following is the overall Dynamic QoS Renegotiation process.

- 1 When a subscriber attaches to the network, the following happens:
 - Dampening timer is started for the subscriber.
 - QoSI is assigned to the subscriber. This becomes the QoSC till a re-negotiation occurs, as shown in the figure below.
 - The traffic class bitfield is cleared.
- 2 As the subscriber starts using some applications, the traffic gets classified on the basis of type of data packets or traffic as mentioned in section *Classification of Application Traffic*. The corresponding bit in the Traffic-class-bitfield is set accordingly.
- 3 The mechanics of QoS renegotiation are as follows:
 - Examine traffic-class-bitfield to determine the highest bit that is set. This gives the desired QoS Traffic Class (QoSD). The associated uplink/downlink peak-data-rate and guaranteed-data-rate values are taken from the configured parameters for this traffic class in the subscriber APN.
 - If QoSC matches QoSD, no QoS renegotiation is required. Otherwise, send an Update PDP Context Request to the SGSN with the QoSD values and QoS renegotiation starts.
 - Reset the dampening timer.
 - Clear the traffic-class-bitfield.
- 4 QoS renegotiation happens under the following conditions:

- When a higher priority traffic is detected, QoS is renegotiated immediately without waiting for the dampening time to expire. For example, if the current traffic has a QoS of Interactive and the system detects streaming traffic, QoS is immediately upgraded to Streaming.
- When lower priority traffic is detected, the system waits for the expiry of the dampening timer before lowering the QoS.
- During "silence" or no-traffic, QoS renegotiation requests are not initiated.

As seen in the following figure, the QoS profile for the subscriber goes through three renegotiations to match the QoS profile of the highest priority application currently being used.

Figure 95: Dynamic QoS Renegotiations



When there is no traffic, traffic class drops to "Background" and the corresponding QoS profile is negotiated as described above.

Network Controlled QoS (NCQoS)

Network-controlled QoS is the method by which the system updates the QoS for a PDP context (primary or secondary) upon receipt of Network Requested Update PDP Context (NRUPC) messages from the GGSN. The system can also activate a new secondary PDP context upon receipt of a Network Requested Secondary PDP Context Activation (NRSPCA) message from the GGSN.

How Network Controlled QoS (NCQoS) Works

The GGSN activates or modifies a bearer whenever a service flow matches a statically provisioned Policy and Charging Control (PCC) rule. The network, based on QoS requirements of the application/service, determines what bearers are needed and either modifies an existing bearer or activates a new one.

Statically provisioned PCC rules, called Network Requested Operation (NRO) rules, are configured as charging rules in the Active Charging Service (ACS). As a part of charging action for such rules, QoS-needed and

corresponding Traffic Flow Template (TFT) packet filters are configured. QoS-needed mainly consists of QoS Class Identifier (QCI) and data rates. Whereas, TFT mainly consists of uplink and downlink packet filter information.

**Warning**

This feature does not work in conjunction with IMS-Authorization service.

When a packet arrives, the ACS analyzes it and performs rule matching based on the priority in the rulebase. If an NRO rule bound to the context on which the packet arrived matches, ACS applies the bandwidth limit and gating. If an NRO rule bound to some other context matches, ACS discards the packet.

If an unbound NRO rule matches, ACS finds a context with the same QCI as the NRO rule, where the context's Maximum Bit Rate (MBR) and matched rule's MBR (context's MBR + matched rule's MBR) is less than the MBR for that QCI in the APN. If such a context is found, NRUPC for that context is triggered. If the request succeeds, the rule will be bound to that context.

**Important**

The packet that triggered the NRUPC request is discarded.

If no context satisfying the MBR limit is found, or if there is no context with the same QCI as the NRO rule, the system triggers NRSPCA. If the request succeeds, the rule is bound to that context.

**Important**

The packet that triggered the NRSPCA request is discarded.

TFTs from the charging-action associated with the NRO rule are also sent as part of the NRUPC/NRSPCA request, and returned as part of the Create PDP Context Response.

Finally, if a non-NRO rule matches, ACS proceeds with the normal processing of that packet. Non-NRO charging-actions can still do "flow action" or ITC (limit-for-flow-type and limit-for-bandwidth).

ACS also does the following:

- Before making an NRUPC/NRSPCA Request, ACS checks if there is any outstanding request for the same QCI for the same subscriber. If there is, it will not process the new request and discards the packet.
- After a context is terminated, ACS unbinds all the rules bound to that context. Such a rule can later be bound to some other context when a packet matches that rule.

**Important**

The packet that triggered the NRUPC/NRSPCA request is discarded.

Configuring Dynamic QoS Renegotiation

This section describes how to configure per-APN based Dynamic QoS Renegotiation.

**Caution**

For Dynamic QoS Renegotiation, two RADIUS attributes are required for remote subscriber configuration. For a particular subscriber, these attributes can be overridden without considering the timeout for Dynamic QoS Renegotiation and whether Dynamic QoS Renegotiation is enabled or not.

To configure Dynamic QoS Renegotiation:

-
- Step 1** Configure an Access Control List (ACL), as described in the [Configuring ACL for Dynamic QoS Renegotiation, on page 692](#) section.
- Step 2** Configure an APN for Dynamic QoS Renegotiation as described in the [Configuring APNs for Dynamic QoS Renegotiation, on page 693](#) section.
- Step 3** Save your configuration as described in *Verifying and Saving Your Configuration*.
- Step 4** Monitor the operations as described in the [Monitoring Dynamic QoS Renegotiation Operation, on page 695](#) section.
- Important** Commands used in the configuration examples in this section reflect base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *ACS Configuration Mode Commands* and *APN Configuration Mode Commands* sections of the *Command Line Interface Reference* for complete information regarding all commands.
-

Configuring ACL for Dynamic QoS Renegotiation

Configuring an ACL and applying it to an APN template are required to specify permission and treatment levels for Dynamic QoS Renegotiation.

Use the following example to configure an ACL for Dynamic QoS Renegotiation:

```
configure
  context <context_name>
    ip access-list <acl_name>
      permit { tcp | udp } ..... treatment { background | conversational | interactive-1 | interactive-2
| interactive-3 | streaming }
    end
```

Notes:

- *context_name* must be the name of the destination context in which you want to configure the ACL. The same context must be used for APN configuration.
- For information on configuring the rules that comprise the ACL, refer to *Access Control Lists*.

Configuring Charging Action for Dynamic QoS Renegotiation

Use the following example to configure charging action parameters for Dynamic QoS Renegotiation support:

```
configure
  active-charging service <service_name>
    charging-action <charging_action_name> -noconfirm
      qos-renegotiate traffic-class streaming
      flow action discard
```



```

    flow limit-for-bandwidth direction downlink peak-data-rate <bps> peak-burst-size <bytes>
violate-action lower-ip-precedence
end

```

Notes:

- A maximum of eight packet filters can be configured per charging action.
- The flow limit-for-bandwidth command contains other option than the example shown here. See *ACS Charging Action Configuration Mode Commands* in the *Command Line Interface Reference* for more information on this command.

Configuring Rulebase for Dynamic QoS Renegotiation

Use the following example to configure rulebase parameters for Dynamic QoS Renegotiation support:

```

configure
  active-charging service <service_name>
    rulebase <rulebase_name> [ -noconfirm ]
    qos-renegotiate timeout <timeout>
  end

```

Configuring APNs for Dynamic QoS Renegotiation

Use the following example to configure an APN template's QoS profile in support of Dynamic QoS Renegotiation:

```

configure
  context <context_name>
    apn <apn_name>
      ip access-group <acl_name> [ in | out ]
    end

```

Notes:

- *context_name* must be the name of the destination context in which you have already configured the ACL, and want to configure the APN template.
- *<acl_name>* must be the name of the ACL that you have already configured in the context.
- If the optional **in** or **out** keywords are not specified in the **ip access-group** command (APN Configuration Mode), the ACL will be applied to all inbound and outbound packets.

Configuring Network Controlled QoS (NCQoS)

To configure NCQoS:

-
- Step 1** Configure packet filter parameters as described in the [Configuring Packet Filter for NCQoS](#), on page 694 section.
 - Step 2** Configure charging rules and actions as described in the [Configuring Charging Action for NCQoS](#), on page 694 section.
 - Step 3** Configure APN template and enable bearer control mode for NCQoS as described in the [Configuring APN for NCQoS](#), on page 695 section.
 - Step 4** Save your configuration as described in *Verifying and Saving Your Configuration*.
 - Step 5** Monitor the operations as described in the [Monitoring Dynamic QoS Renegotiation Operation](#), on page 695 section.
-
- Important** Commands used in the configuration examples in this section implement base functionality (most common or likely commands and/or keyword options). In many cases, other commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.
-

Configuring Packet Filter for NCQoS

Use the following example to configure packet filter parameters for NCQoS support:

```
configure
  active-charging service <service_name>
    packet-filter <filter_name> [ -noconfirm ]
      ip local-port { = <port_num> | range <start_port_num> to <end_port_num> }
      ip protocol { = <proto_num> | range <start_proto_num> to <end_proto_num> }
      ip remote-address { = { <ip_address> | <ip_address/mask> } | { range { <ip_address> |
<ip_address/mask> } to { <ip_address> | <ip_address/mask> } } }
      ip remote-port { = <port_num> | range <start_port_num> to <end_port_num> }
      direction { bi-directional | download | upload }
      priority <priority>
    end
```

Configuring Charging Action for NCQoS

Use the following example to configure charging action parameters for NCQoS support:

```
configure
  active-charging service <service_name>
    charging-action <charging_action_name> [ -noconfirm ]
      qos-class-identifier <identifier>
      flow action discard [ downlink | uplink ]
      tft packet-filter <filter_name>
      flow limit-for-bandwidth direction { downlink | uplink } peak-data-rate <bps> peak-burst-size
<bytes> violate-action { discard | lower-ip-precedence }
    end
```

Notes:

- A number of optional keywords and variable are available for the **flow limit-for-bandwidth direction** command. Refer to the *ACS Charging Action Configuration Mode Commands* section of the *Command Line Interface Reference* for more information regarding this command.

Configuring APN for NCQoS

Use the following example to enable Bearer Control Mode (BCM) for NCQoS support:

```
configure
context <context_name>
  apn <apn_name>
    bearer-control-mode [ mixed | ms-only | none ]
  end
```

Notes:

- To enable NCQoS, bearer-control-mode in the APN Configuration Mode must be configured with **mixed** mode.

Monitoring Dynamic QoS Renegotiation Operation

Use the following steps to verify/monitor Dynamic QoS Renegotiation operations:

-
- Step 1** Verify that your APNs were configured properly by entering the following command:
show apn { all | name apn_name }
 The output is a listing of APN parameter settings.
- Step 2** Verify that the ACLs have been properly applied by entering the following command:
show apn name apn_name
apn_name must be the name of the APN configured in the *Configuring APNs for Dynamic QoS Renegotiation* section. The output of this command displays the APN configuration. Examine the output for the **ip output access-group** and **ip input access-group** fields. For more details refer to the *Applying a Single ACL to Multiple Subscribers* section.
- Step 3** Verify that your ACL was configured properly by entering the following command:
show ip access-list acl_name
 The output is a concise listing of IP Access Control List parameter settings.
- Step 4** Monitor your QoS renegotiation status for a subscriber by running the **show subscriber ggsn-only full** command (Exec mode).
 The output is a concise listing of subscribers' settings.
- Step 5** For L7 based QoS Renegotiation, view how many time QoS renegotiations have happened for that session by running the **show active-charging sessions full all** command (Exec mode).
- Step 6** View the statistics of APN related to QoS renegotiation parameters by entering the following command:
show apn statistics { all | name apn_name }
 The output is a listing of APN statistics related to QoS Renegotiation.
-

Event IDs Pertaining to Dynamic QoS Renegotiation

The Session Manager facility sources event IDs that can be useful for diagnosing errors that could occur when implementing of Dynamic QoS Renegotiation feature.

The following table displays information pertaining to these events.

Table 53: Event IDs in Session Manager Pertaining to Dynamic QoS Renegotiation

Event	Event ID	Type	Additional Information
QoS Renegotiation timer started for subscriber	10917	Info	"Indicates that the Dynamic QoS Renegotiation timer was started for the subscriber"
QoS Renegotiation timer stopped for subscriber	10918	Info	"Indicates that the Dynamic QoS Renegotiation timer was stopped for the subscriber"
QoS Renegotiation timer expired for subscriber	10919	Info	"Indicates that the Dynamic QoS Renegotiation timer was expired for the subscriber"
QoS Renegotiation message sent for subscriber	10920	Info	"Indicates that the Dynamic QoS Renegotiation message was sent for the subscriber"
L4 classification done for subscriber traffic	10921	Info	"Indicates the kind of L4 classification that was done for the subscriber traffic."

RADIUS Attributes

The RADIUS attributes listed in the following table are used to enable Dynamic QoS Renegotiation for subscribers configured on remote RADIUS servers.

For more information on these attributes, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Table 54: RADIUS Attributes Required for Dynamic QoS Renegotiation Support

Attribute	Description
SN-Enable-QoS-Renegotiation (or SN1-Enable-QoS-Renegotiation)	Enables the Dynamic QoS Renegotiation for specific profile application. This attribute displays "enable qos renegotiation".
SN-QoS-Renegotiation-Timeout (or SN1-QoS-Renegotiation-Timeout)	Timeout duration for dampening time for QoS renegotiation to specific profile application. This attribute displays "qos renegotiation timeout".



Remote Address-based RADIUS Accounting

This chapter provides information on configuring an enhanced, or extended, service. The product administration guides provide examples and procedures for the configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

This chapter includes the following topics:

- [Overview, page 697](#)
- [Configuring Remote Address-based Accounting, page 698](#)
- [Subscriber Attribute Configuration, page 698](#)

Overview

Remote address-based RADIUS accounting counts the number of octets exchanged between individual subscribers and specific remote IP addresses, or networks, during a packet data session. Data from the subscriber to the remote addresses, and data from the remote addresses to the subscriber are accounted for separately.

The remote addresses for which to collect RADIUS accounting data are configured in lists on a per-context basis. Individual subscribers are associated with particular address lists through the configuration or specification of an attribute in their locally configured or RADIUS server-based profiles. Once the lists and subscriber profiles are configured, accounting data collection can be enabled on the system.

Remote address-based RADIUS accounting is implemented in the system according to the specifications described in TIA/EIA/IS-835-B, CDMA2000 Wireless IP Network Standard, October 2002 and 3GPP2 X.S0011-005-D.

License Requirements

The Remote address-based RADIUS Accounting is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter in the *System Administration Guide*.

Configuring Remote Address-based Accounting

To configure this functionality, a list of up to ten remote addresses or networks is configured in the authentication context, the list is assigned to a subscriber, and remote address collection is enabled.

Use the following configuration example to configure remote address-based accounting:

```
configure
  context <context_name>
    radius group <group_name>
    radius accounting ip remote-address list <list_id>
    address <ipv4_address/ipv6_address> netmask <netmask>
  end
```

Verifying the Remote Address Lists

Use the following command to verify the remote address lists:

```
show configuration context <context_name>
```

Output similar to the following is displayed.

```
[local] host_name show configuration context <context_name>
configure
  context <context_name>
    subscriber default
    exit
  radius accounting ip remote-address list 1
    address <ipv4_address/ipv6_address> netmask <netmask>
    address <ipv4_address/ipv6_address> netmask <netmask>
    address <ipv4_address/ipv6_address> netmask <netmask>
  end
```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Subscriber Attribute Configuration

Subscriber attributes are configured as part of their profile. Subscriber profiles can be configured either remotely on a RADIUS server or locally on the system.

This section provides information and procedures on the attributes used to support this functionality.



Important

Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Please refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

Supported RADIUS Attributes

The following RADIUS attributes are used to configure remote address-based RADIUS accounting for a subscriber session. For specific information on each attribute, if you are using StarOS 12.3 or an earlier release, see the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

- 3GPP2-Remote-Addr-Table-Index
- 3GPP2-Remote-IPv4-Address
- 3GPP2-Remote-IPv4-Addr-Octets

Configuring Local Subscriber Profiles

Use the following example to configure local subscriber profiles to support the Remote Address-based RADIUS Accounting feature:

```
configure
  context <context_name>
    subscriber name <name>
      radius accounting ip remote-address list-id <list_id>
    end
  end
configure
  context <context_name>
    radius accounting ip remote-address collection
  end
```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.



CHAPTER 36

Routing Behind the Mobile Station on an APN

The following rules apply:

- AAA interface of GGSN/P-GW supports receiving "Framed Route AVP" in Radius Access-Accept Message from the Radius Server.
- AAA interface of GGSN/P-GW supports maximum 16 "Framed Route AVP" in Radius Access-Accept Message
- GGSN/P-GW does not accept framed route with destination address as 0.0.0.0 and/or netmask as 0.0.0.0.
- GGSN/P-GW does not accept framed route where gateway address in the route is not matching with the address that would be assigned to Mobile station.
- GGSN/P-GW ignores duplicate framed routes.
- GGSN/P-GW supports controlling enabling/disabling of this feature through CLI in APN Configuration.
- GGSN/P-GW supports controlling number of framed-routes to be installed through this feature.
- GGSN/P-GW supports controlling number of hosts (addresses) supported behind the mobile station per route.
- The routing behind an MS is supported only for IPv4 PDP contexts.
- Packets routed behind the MS share the same 3GPP QoS settings of the MS.
- [Feature Description, page 701](#)
- [How It Works, page 702](#)
- [Configuring Routing Behind the Mobile Station, page 702](#)
- [Monitoring and Troubleshooting the Routing Behind the Mobile Station, page 707](#)

Feature Description

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message. Framed-Route can work at a context level or VRF level. VRFs can be on per enterprise and each can have its

own set of framed-routes. In such configuration, framed routes will be installed in VRF's dedicated for respective enterprise. Association of Framed-Route with VRF will be done based on subscriber IP pool.

Mobile Router enables a router to create a PDN Session which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the "mobile router." If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN session.

How It Works

Routing Behind the Mobile Station on an APN

The following rules apply:

- AAA interface of GGSN/P-GW supports receiving "Framed Route AVP" in Radius Access-Accept Message from the Radius Server.
- AAA interface of GGSN/P-GW supports maximum 16 "Framed Route AVP" in Radius Access-Accept Message
- GGSN/P-GW does not accept framed route with destination address as 0.0.0.0 and/or netmask as 0.0.0.0.
- GGSN/P-GW does not accept framed route where gateway address in the route is not matching with the address that would be assigned to Mobile station.
- GGSN/P-GW ignores duplicate framed routes.
- GGSN/P-GW supports controlling enabling/disabling of this feature through CLI in APN Configuration.
- GGSN/P-GW supports controlling number of framed-routes to be installed through this feature.
- GGSN/P-GW supports controlling number of hosts (addresses) supported behind the mobile station per route.
- The routing behind an MS is supported only for IPv4 PDP contexts.
- Packets routed behind the MS share the same 3GPP QoS settings of the MS.

Configuring Routing Behind the Mobile Station

The routing behind the MS feature enables the routing of packets to IPv4 addresses that do not belong to the PDN Session (the MS), but exist behind it. The network address of the destination can be different than the MS address.

Before enabling routing behind the MS, the following requirements must be met:

- The MS must use RADIUS for authentication and authorization.
- The Framed-Route (attribute 22) as defined in Internet Engineering Task Force (IETF) standard RFC 2865, must be configured in the profile of a user and contain at least one route, and up to 16 routes for each MS that is to use the routing behind the MS feature.

When configured, the Framed-Route attribute is automatically downloaded to the GGSN during the RADIUS authentication and authorization phase of the PDN Session creation. If routing behind the MS has not been enabled using the `network-behind-mobile` command in access-point configuration mode, the GGSN ignores the Framed-Route attribute.

When the MS session is no longer active, the routes are deleted.

- Static routes are not configured. The configuration of the routing behind the mobile station feature (Framed Route, attribute 22) and static routes at the same time is not supported.

Configuration Overview

To enable routing behind a Mobile Station perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Create an APN Profile. Refer to Creating an APN Profile , on page 703. |
| Step 2 | Enable or disable a Network behind Mobile Station for APN. Refer to Enabling Routing Behind the Mobile Station , on page 703. |
-

Creating an APN Profile

Use the following example to create an APN profile on the P-GW/SAEGW/S-GW:

```
config
context context_name
  apn apn_name
end
```

Notes:

- The apn name must be an alphanumeric string from 1 to 64 characters in length.
- Once you have created an APN profile, you will enter the Access Point Profile Configuration Mode.

Enabling Routing Behind the Mobile Station

To enable routing behind an MS, use the following steps command in access-point configuration mode:

```
config
network-behind-mobile { max-addresses-behind-mobile max_addrs | max-subnets max_subnets }
{ default | no } network-behind-mobile
end
```

Notes:

- **default**
Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.
- **no**
Disables the network behind mobile station functionality on the APN.

- **max-addresses-behind-mobile** *max_addr*
Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.
- **max-subnets** *max_subnets*
Specifies the maximum number of subnets that can be enabled for a call in the APN.
max_subnets must be an integer from 1 through 16.
Default: 10

Verifying the Routing Behind the Mobile Station

To verify the routing behind the mobile station configuration, use the following show commands.

```

1 Router show ip route vrf vpn_am2
   "*" indicates the Best or Used route.  S indicates Stale.
   Destination      Nexthop      Protocol  Prec Cost  Interface
   *17.18.19.20/32   10.7.104.2   bgp       20  0    bgp_neighbour
   (nhlfe-ix:3)
   *17.18.19.21/32   0.0.0.0      connected  0   0    vpn_am21b1
   *40.40.41.0/24    0.0.0.0      connected  0   0
   *41.40.41.0/24    0.0.0.0      connected  0   0
   *42.40.41.0/24    0.0.0.0      connected  0   0
   *43.40.41.0/24    0.0.0.0      connected  0   0
   *44.40.41.0/24    0.0.0.0      connected  0   0
   *45.40.41.0/24    0.0.0.0      connected  0   0
   *46.40.41.0/24    0.0.0.0      connected  0   0
   *47.40.41.0/24    0.0.0.0      connected  0   0
   *48.40.41.0/24    0.0.0.0      connected  0   0
   *49.40.41.0/24    0.0.0.0      connected  0   0
   *106.106.0.0/16   0.0.0.0      connected  0   0    pool pool_test_3
   Total route count : 13
   Unique route count: 13
   Connected: 12 BGP: 1

2 show subscribers pgw-only full all
   Username: starent
   Subscriber Type : Visitor
   Status          : Online/Active
   State           : Connected
   Connect Time    : Mon Oct 12 12:23:52 2015
   Auto Delete     : No
   Idle time       : 00h00m50s
   MS TimeZone     : n/a
   Access Type: gtp-pdn-type-ipv4
   Access Tech: eUTRAN
   Callid: 0db5d3a3
   Protocol Username: starent
   Interface Type: S5S8GTP
   Emergency Bearer Type: N/A
   IMS-media Bearer: No
   S6b Auth Status: N/A
   Access Peer Profile: default
   Acct-session-id (C1): 141414650F55554B
   ThreeGPP2-correlation-id (C2): 17767C4D / 6SKDhW-2
   Card/Cpu: 12/0
   Bearer Type: Default
   Bearer State: Active
   IP allocation type: local pool
   IPv6 allocation type: N/A
   IP address: 106.106.0.5
   Framed Routes:
   40.40.41.0      255.255.255.0  106.106.0.5
   41.40.41.0      255.255.255.0  106.106.0.5
   43.40.41.0      255.255.255.0  106.106.0.5
   44.40.41.0      255.255.255.0  106.106.0.5
   45.40.41.0      255.255.255.0  106.106.0.5
   46.40.41.0      255.255.255.0  106.106.0.5
   47.40.41.0      255.255.255.0  106.106.0.5
   48.40.41.0      255.255.255.0  106.106.0.5
   49.40.41.0      255.255.255.0  106.106.0.5
   42.40.41.0      255.255.255.0  106.106.0.5
   ULI:
   TAI-ID:
   MCC: 214 MNC: 365
   TAC: 0x6789
   ECGI-ID:
   MCC: 214 MNC: 365
   ECI: 0x1234567
   Accounting mode: None
   MEI: 1122334455667788
   charging id: 257250635
   Source context: EPC2
   S5/S8/S2b/S2a-APN: cisco.com
   SGI-APN: cisco.com
   APN-OI: n/a
   Restoration priority level: n/a
   Daylight Saving Time: n/a
   Network Type: IP
   pgw-service-name: PGW21
   IMSI: 123456789012345
   MSISDN: 9326737733
   Low Access Priority: N/A
   Sessmgr Instance: 47
   Bearer-Id: 5
   Framed Routes Source: RADIUS
   APN Selection Mode: Sent by MS
   Serving Nw: MCC=123, MNC=765
   charging chars: normal
   Destination context: ISP1

```

```

    traffic flow template: none
    IMS Auth Service : IMSGx
    active input ipv4 acl: IPV4ACL
    active input ipv6 acl:
    ECS Rulebase: cisco
    Bearer QoS:
    QCI: 5
    ARP: 0x04
    PCI: 0 (Enabled)
    PL : 1
    PVI: 0 (Enabled)
    MBR Uplink(bps): 0
    GBR Uplink(bps): 0
    PCRF Authorized Bearer QoS:
    QCI: n/a
    ARP: n/a
    PCI: n/a
    PL: n/a
    PVI: n/a
    MBR uplink (bps): n/a
    GBR uplink (bps): n/a
    Downlink APN AMBR: n/a
    P-CSCF Address Information:
    Primary IPv6 : n/a
    Secondary IPv6: n/a
    Tertiary IPv6 : n/a
    Primary IPv4 : n/a
    Secondary IPv4: n/a
    Tertiary IPv4 : n/a
    Access Point MAC Address: N/A
    pgw c-teid: [0x8000002f] 2147483695
    sgw c-teid: [0x50010001] 1342242817
    ePDG c-teid: N/A
    cgw c-teid: N/A
    pgw c-addr: 2002::2:101
    sgw c-addr: 2002::2:61
    ePDG c-addr: N/A
    cgw c-addr: N/A
    Downlink APN AMBR: 16534000 bps
    Mediation context: None
    Mediation No Interims: Disabled
    input pkts: 0
    input bytes: 0
    input bytes dropped: 0
    input pkts dropped: 0
    input pkts dropped due to lorc : 0
    0
    input bytes dropped due to lorc : 0
    in packet dropped suspended state: 0
    in bytes dropped suspended state: 0
    in packet dropped overcharge protection: 0
    0
    in bytes dropped overcharge protection: 0
    0
    in packet dropped sgw restoration state: 0
    state: 0
    in bytes dropped sgw restoration state: 0
    0
    pk rate from user(bps): 0
    ave rate from user(bps): 0
    sust rate from user(bps): 0
    pk rate from user(pps): 0
    ave rate from user(pps): 0
    sust rate from user(pps): 0
    link online/active percent: 65
    ipv4 bad hdr: 0
    ipv4 fragments sent: 0
    ipv4 input acl drop: 0
    ipv4 bad length trim: 0
    ipv4 input mcast drop: 0
    ipv6 input acl drop: 0
    ipv4 input css down drop: 0
    ipv4 input css down drop: 0

    active output ipv4 acl: IPV4ACL
    active output ipv6 acl:
    MBR Downlink(bps): 0
    GBR Downlink(bps): 0
    MBR downlink (bps): n/a
    GBR downlink (bps): n/a
    Uplink APN AMBR: n/a
    pgw u-teid: [0x8000002f] 2147483695
    sgw u-teid: [0x60010001] 1610678273
    ePDG u-teid: N/A
    cgw u-teid: N/A
    pgw u-addr: 20.20.20.101 2002::2:101
    sgw u-addr: 2002::2:61
    ePDG u-addr: N/A
    cgw u-addr: N/A
    Uplink APN AMBR: 16534000 bps
    Mediation no early PDUs: Disabled
    Mediation Delay PBA: Disabled
    output pkts: 0
    output bytes: 0
    output bytes dropped: 0
    output pkts dropped: 0
    output pkts dropped due to lorc :
    out packet dropped suspended state: 0
    out bytes dropped suspended state: 0
    out packet dropped overcharge protection:
    out bytes dropped overcharge protection:
    out packet dropped sgw restoration
    out bytes dropped sgw restoration state:
    pk rate to user(bps): 0
    ave rate to user(bps): 0
    sust rate to user(bps): 0
    pk rate to user(pps): 0
    ave rate to user(pps): 0
    sust rate to user(pps): 0
    ipv4 ttl exceeded: 0
    ipv4 could not fragment: 0
    ipv4 output acl drop: 0
    ipv4 input bcast drop: 0
    ipv6 output acl drop: 0
    ipv4 output css down drop: 0
    ipv4 output css down drop: 0

```

```

    ipv4 output xoff pkts drop: 0
    ipv6 output xoff pkts drop: 0
    ipv6 input ehrpd-access drop: 0
input pkts dropped (0 mbr): 0
    ip source violations: 0
    ipv6 egress filtered: 0
    ipv4 proxy-dns redirect: 0
    ipv4 proxy-dns drop: 0
    ipv4 proxy-dns redirect tcp connection: 0
    ipv6 bad hdr: 0
    ip source violations no acct: 0
    ip source violations ignored: 0
    dormancy total: 0
    ipv4 icmp packets dropped: 0
    APN AMBR Input Pkts Drop: 0
    APN AMBR Input Bytes Drop: 0

    ipv4 output xoff bytes drop: 0
    ipv6 output xoff bytes drop: 0
    ipv6 output ehrpd-access drop: 0
output pkts dropped (0 mbr): 0
    ipv4 output no-flow drop: 0

    ipv4 proxy-dns pass-thru: 0

    ipv6 bad length trim: 0

    handoff total: 0

    APN AMBR Output Pkts Drop: 0
    APN AMBR Output Bytes Drop: 0

```

Monitoring and Troubleshooting the Routing Behind the Mobile Station

Routing Behind the Mobile Station Show Command(s) and/or Outputs

show apn name <apn_name>

```

...
proxy-mip: Disabled
proxy-mipv6: Disabled
proxy-mip null-username static home address: Disabled
Network Behind Mobile Station: Enabled
Maximum subnets behind Mobile station: 10
Maximum Addresses Behind Mobile Station: 16777214
Tunnel peer load-balancing : random
L3-to-L2 tunnel address-policy no-alloc-validate
tunnel address-policy alloc-validate
NPU QoS Traffic Priority: Derive from packet DSCP

```




Rf Interface Support

This chapter provides an overview of the Diameter Rf interface and describes how to configure the Rf interface.

Rf interface support is available on the Cisco system running StarOS 10.0 or later releases for the following products:

- Gateway GPRS Support Node (GGSN)
- Proxy Call Session Control Function (P-CSCF)
- Packet Data Network Gateway (P-GW)
- Serving Call Session Control Function (S-CSCF)



Important

In StarOS version 19 and later releases, the Rf interface is not supported on the S-GW.

It is recommended that before using the procedures in this chapter you select the configuration example that best meets your service model, and configure the required elements for that model as described in the administration guide for the product that you are deploying.

This chapter includes the following topics:

- [Introduction, page 709](#)
- [Features and Terminology, page 713](#)
- [How it Works, page 727](#)
- [Configuring Rf Interface Support, page 729](#)

Introduction

The Rf interface is the offline charging interface between the Charging Trigger Function (CTF) (for example, P-GW, P-CSCF) and the Charging Collection Function (CCF). The Rf interface specification for LTE/GPRS/eHRPD offline charging is based on 3GPP TS 32.299 V8.6.0, 3GPP TS 32.251 V8.5.0 and other 3GPP specifications. The Rf interface specification for IP Multimedia Subsystem (IMS) offline charging is based on 3GPP TS 32.260 V8.12.0 and 3GPP TS 32.299 V8.13.0.

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows the CTF (Diameter client) to issue offline charging events to a Charging Data Function (CDF) (Diameter server). The charging events can either be one-time events or may be session-based.

The system provides a Diameter Offline Charging Application that can be used by deployed applications to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on chassis to act as CTF to a configured CDF.

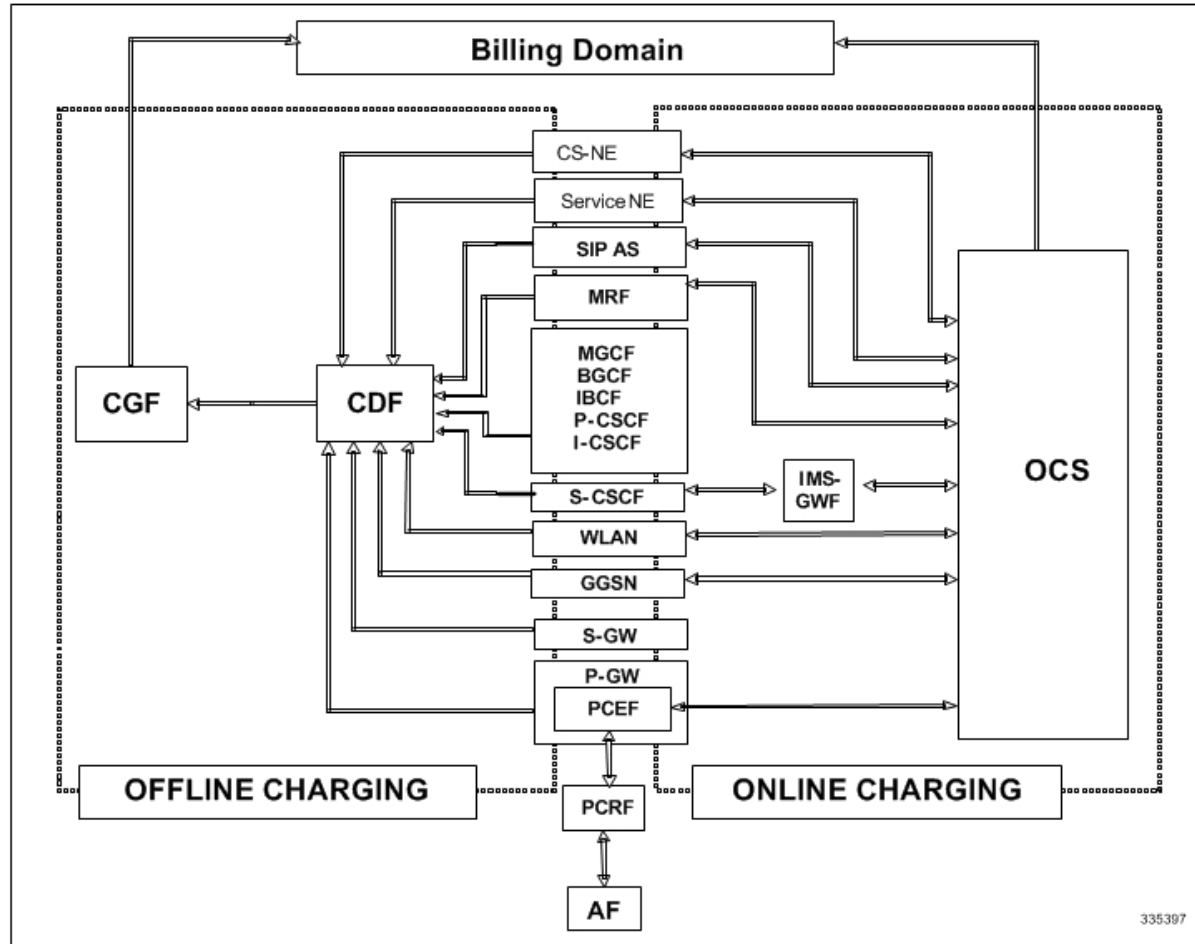
In general, accounting information from core network elements is required to be gathered so that the billing system can generate a consolidated record for each rendered service.

The CCF with the CDF and Charging Gateway Function (CGF) will be implemented as part of the core network application. The CDF function collects and aggregates Rf messages from the various CTFs and creates CDRs. The CGF collects CDRs from the CDFs and generates charging data record files for the data mediation/billing system for billing.

Offline Charging Architecture

The following diagram provides the high level charging architecture as specified in 3GPP 32.240. The interface between CSCF, P-GW and GGSN with CCF is Rf interface. Rf interface for EPC domain is as per 3GPP standards applicable to the PS Domain (e.g. 32.240, 32.251, 32.299, etc.).

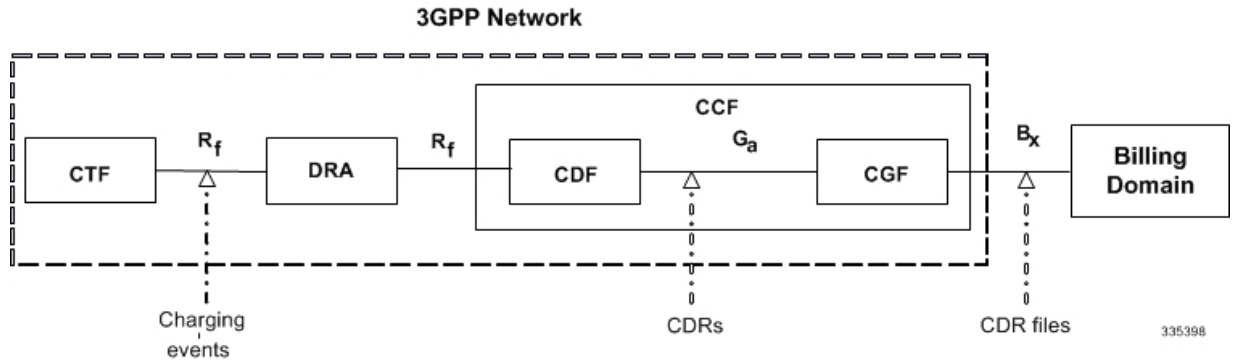
Figure 96: Charging Architecture



335397

The following figure shows the Rf interface between CTF and CDF.

Figure 97: Logical Offline Charging Architecture



The Rf offline charging architecture mainly consists of three network elements CCF, CTF and Diameter Dynamic Routing Agent (DRA).

Charging Collection Function

The CCF implements the CDF and CGF. The CCF will serve as the Diameter Server for the Rf interface. All network elements supporting the CTF function should establish a Diameter based Rf Interface over TCP connections to the DRA. The DRA function will establish Rf Interface connection over TCP connections to the CCF.

The CCF is primarily responsible for receipt of all accounting information over the defined interface and the generation of CDR (aka UDRs and FDRs) records that are in local storage. This data is then transferred to the billing system using other interfaces. The CCF is also responsible for ensuring that the format of such CDRs is consistent with the billing system requirements. The CDF function within the CCF generates and CGF transfers the CDRs to the billing system.

The CDF function in the CCF is responsible for collecting the charging information and passing it on to the appropriate CGF via the GTP' based interface per 3GPP standards. The CGF passes CDR files to billing mediation via SCP.

Charging Trigger Function

The CTF will generate CDR records and passes it onto CCF. When a P-GW service is configured as CTF, then it will generate Flow Data Record (FDR) information as indicated via the PCRF. The P-GW generates Rf messages on a per PDN session basis. There are no per UE or per bearer charging messages generated by the P-GW.

The service data flows within IP-CAN bearer data traffic is categorized based on a combination of multiple key fields (Rating Group, Rating Group and Service-Identifier). Each Service-Data-Container captures single bi-directional flow or a group of single bidirectional flows as defined by Rating Group or Rating Group and Service-Identifier.

Dynamic Routing Agent

The DRA provides load distribution on a per session basis for Rf traffic from CTFs to CCFs. The DRA acts like a Diameter Server to the Gateways. The DRA acts like a Diameter client to CCF. DRA appears to be a CCF to the CTF and as a CTF to the CCF.

The DRA routes the Rf traffic on a per Diameter charging session basis. The load distribution algorithm can be configured in the DRA (Round Robin, Weighted distribution, etc). All Accounting Records (ACRs) in one Diameter charging session will be routed by the DRA to the same CCF. Upon failure of one CCF, the DRA selects an alternate CCF from a pool of CCFs.

License Requirements

The Rf interface support is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Supported Standards

Rf interface support is based on the following standards:

- IETF RFC 4006: Diameter Credit Control Application; August 2005
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release9)

Features and Terminology

This section describes features and terminology pertaining to Rf functionality.

Offline Charging Scenarios

Offline charging for both events and sessions between CTF and the CDF is performed using the Rf reference point as defined in 3GPP TS 32.240.

Basic Principles

The Diameter client and server must implement the basic functionality of Diameter accounting, as defined by the RFC 3588 Diameter Base Protocol.

For offline charging, the CTF implements the accounting state machine as described in RFC 3588. The CDF server implements the accounting state machine "SERVER, STATELESS ACCOUNTING" as specified in RFC 3588, i.e. there is no order in which the server expects to receive the accounting information.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the following ACR event types:

Table 55: Rf ACR Event Types

Request	Description
START	Starts an accounting session
INTERIM	Updates an accounting session
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event

ACR types START, INTERIM and STOP are used for accounting data related to successful sessions. In contrast, EVENT accounting data is unrelated to sessions, and is used e.g. for a simple registration or interrogation and successful service event triggered by a network element. In addition, EVENT accounting data is also used for unsuccessful session establishment attempts.



Important

The ACR Event Type "EVENT" is supported in Rf CDRs only in the case of IMS specific Rf implementation.

The following table describes all possible ACRs that might be sent from the IMS nodes i.e. a P-CSCF and S-CSCF.

Table 56: Accounting Request Messages Triggered by SIP Methods or ISUP Messages for P-CSCF and S-CSCF

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Start]	SIP 200 OK acknowledging an initial SIP INVITE
	ISUP:ANM (applicable for the MGCF)
ACR [Interim]	SIP 200 OK acknowledging a SIP
	RE-INVITE or SIP UPDATE [e.g. change in media components]
	Expiration of AVP [Acct-Interim-Interval]
	SIP Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP RE-INVITE or SIP UPDATE
ACR [Stop]	SIP BYE message (both normal and abnormal session termination cases)
	ISUP:REL (applicable for the MGCF)

Diameter Message	Triggering SIP Method/ISUP Message
ACR [Event]	SIP 200 OK acknowledging non-session related SIP messages, which are: <ul style="list-style-type: none"> • SIP NOTIFY • SIP MESSAGE • SIP REGISTER • SIP SUBSCRIBE • SIP PUBLISH
	SIP 200 OK acknowledging an initial SIP INVITE
	SIP 202 Accepted acknowledging a SIP REFER or any other method
	SIP Final Response 2xx (except SIP 200 OK)
	SIP Final/Redirection Response 3xx
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful SIP session set-up
	SIP Final Response (4xx, 5xx or 6xx), indicating an unsuccessful session-unrelated procedure
	SIP CANCEL, indicating abortion of a SIP session set-up

Event Based Charging

In the case of event based charging, the network reports the usage or the service rendered where the service offering is rendered in a single operation. It is reported using the ACR EVENT.

In this scenario, CTF asks the CDF to store event related charging data.

Session Based Charging

Session based charging is the process of reporting usage reports for a session and uses the START, INTERIM & STOP accounting data. During a session, a network element may transmit multiple ACR Interims' depending on the proceeding of the session.

In this scenario, CTF asks the CDF to store session related charging data.

Diameter Base Protocol

The Diameter Base Protocol maintains the underlying connection between the Diameter Client and the Diameter Server. The connection between the client and server is TCP based.

In order for the application to be compliant with the specification, state machines should be implemented at some level within the implementation.

Diameter Base supports the following Rf message commands that can be used within the application.

Table 57: Diameter Rf Messages

Command Name	Source	Destination	Abbreviation
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

There are a series of other Diameter messages exchanged to check the status of the connection and the capabilities.

- **Capabilities Exchange Messages:** Capabilities Exchange Messages are exchanged between the diameter peers to know the capabilities of each other and identity of each other.
 - **Capabilities Exchange Request (CER):** This message is sent from the client to the server to know the capabilities of the server.
 - **Capabilities Exchange Answer (CEA):** This message is sent from the server to the client in response to the CER message.
- **Device Watchdog Request (DWR):** After the CER/CEA messages are exchanged, if there is no more traffic between peers for a while, to monitor the health of the connection, DWR message is sent from the client. The Device Watchdog timer (Tw) is configurable and can vary from 6 through 30 seconds. A very low value will result in duplication of messages. The default value is 30 seconds. On two consecutive expiries of Tw without a DWA, the peer is considered to be down.



Important

DWR is sent only after Tw expiry after the last message that came from the server. Say if there is continuous exchange of messages between the peers, DWR might not be sent if (Current Time - Last message received time from server) is less than Tw.

- **Device Watchdog Answer (DWA):** This is the response to the DWR message from the server. This is used to monitor the connection state.
- **Disconnect Peer Request (DPR):** This message is sent to the peer to inform to shutdown the connection. There is no capability currently to send the message to the Diameter server.
- **Disconnect Peer Answer (DPA):** This message is the response to the DPR request from the peer. On receiving the DPR, the peer sends DPA and puts the connection state to "DO NOT WANT TO TALK TO YOU" state and there is no way to get the connection back except for reconfiguring the peer again. A timeout value for retrying the disconnected peer must be provided.

Timer Expiry Behavior

Upon establishing the Diameter connection, an accounting interim timer (AII) is used to indicate the expiration of a Diameter accounting session, and is configurable at the CTF. The CTF indicates the timer value in the ACR-Start, in the Acct-Interim-Interval AVP. The CDF responds with its own AII value (through the DRA), which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. An instance of the AII timer is started in the CCF at the beginning of the accounting session, reset on the receipt of an ACR-Interim and stopped on the receipt of the ACR-Stop. After expiration of the AII timer, ACR INTERIM message will be generated and the timer will be reset and the accounting session will be continued.

Rf Interface Failures/Error Conditions

The current architecture allows for primary and secondary connections or Active-Active connections for each network element with the CDF elements.

DRA/CCF Connection Failure

When the connection towards one of the primary/Active DRAs in CCF becomes unavailable, the CTF picks the Secondary/Active IP address and begins to use that as a Primary.

If no DRA (and/or the CCF) is reachable, the network element must buffer the generated accounting data in non-volatile memory. Once the DRA connection is up, all accounting messages must be pulled by the CDF through offline file transfer.

No Reply from CCF

In case the CTF/DRA does not receive an ACA in response to an ACR, it may retransmit the ACR message. The waiting time until a retransmission is sent, and the maximum number of repetitions are both configurable by the operator. When the maximum number of retransmissions is reached and still no ACA reply has been received, the CTF/DRA sends the ACRs to the secondary/alternate DRA/CCF.

Detection of Message Duplication

The Diameter client marks possible duplicate request messages (e.g. retransmission due to the link failover process) with the T-flag as described in RFC 3588.

If the CDF receives a message that is marked as retransmitted and this message was already received, then it discards the duplicate message. However, if the original of the re-transmitted message was not yet received, it is the information in the marked message that is taken into account when generating the CDR. The CDRs are marked if information from duplicated message(s) is used.

CCF Detected Failure

The CCF closes a CDR when it detects that expected Diameter ACRs for a particular session have not been received for a period of time. The exact behavior of the CCF is operator configurable.

Rf-Gy Synchronization Enhancements

Both Rf (OFCS) and Gy (OCS) interfaces are used for reporting subscriber usage and billing. Since each interface independently updates the subscriber usage, there are potential scenarios where the reported information is not identical. Apart from Quota enforcement, OCS is utilized for Real Time Reporting (RTR), which provides a way to the user to track the current usage and also get notifications when a certain threshold is hit.

In scenarios where Rf (OFCS) and Gy (OCS) have different usage information for a subscriber session, it is possible that the subscriber is not aware of any potential overages until billed (scenario when Rf is more than Gy) or subscriber believes he has already used up the quota whereas his actual billing might be less (scenario when Gy is more than Rf). In an attempt to align both the Rf and Gy reported usage values, release 12.3 introduced capabilities to provide a way to get the reported values on both the interfaces to match as much as possible. However, some of the functionalities were deferred and this feature implements the additional enhancements.

In release 15.0 when time/volume quota on the Gy interface gets exhausted, Gy triggers "Service Data Volume Limit" and "Service Data Time Limit". Now in 16.0 via this feature, this behavior is CLI controlled. Based on the CLI command "**trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit { cache | immediate } }**" the behavior will be decided whether to send the ACR-Interim immediately or to cache the containers for future transactions. If the CLI for the event-triggers received via Gy is not configured, then those ACR-Interims will be dropped.

Releases prior to 16.0, whenever the volume/time-limit event triggers are generated, ACR-Interims were sent out immediately. In 16.0 and later releases, CLI configuration options are provided in policy accounting configuration to control the various Rf messages (ACRs) triggered for sync on this feature.

This release supports the following enhancements:

- Caches containers in scenarios when ACR-I could not be sent and reported to OFCS.
- Triggers ACR to the OFCS when the CCR to the OCS is sent instead of the current implementation of waiting for CCA from OCS.

If an ACR-I could not be sent to the OFCS, the PCEF caches the container record and sends it in the next transaction to the OFCS.

In releases prior to 16.0, once a CCR-U was sent out over Gy interface, ACR-I message was immediately triggered (or containers were cached) based on policy accounting configuration and did not wait for CCA-U. In 16.0 and later releases, the containers are closed only after receiving CCA-U successfully. That is, Rf trigger will be sent only after receiving CCA-U message.

For more information on the command associated with this feature, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

In 17.0 and later releases, a common timer based approach is implemented for Rf and Gy synchronization. As part of the new design, Gy and Rf will be check-pointed at the same point of time for periodic as well as for full check-pointing. Thus, the billing records will always be in sync at all times regardless of during an ICSR switchover event, internal events, session manager crashes, inactive Rf/Gy link, etc. This in turn avoids any billing discrepancies.

Cessation of Rf Records When UE is IDLE

Releases prior to 16.0, when the UE was identified to be in IDLE state and not sending any data, the P-GW generated Rf records. During this scenario, the generated Rf records did not include Service Data Containers (SDCs).

In 16.0 and later releases, the Rf records are not generated in this scenario. New CLI configuration command **"session idle-mode suppress-interim"** is provided to enable/disable the functionality at the ACR level to control the behavior of whether an ACR-I needs to be generated or not when the UE is idle and no data is transferred.

That is, this CLI configuration is used to control sending of ACR-I records when the UE is in idle mode and when there is no data to report.

For more information on the command, see the *Accounting Policy Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

QoS Change Scenarios

QOS_CHANGE Trigger in Rf Records During eHRPD-LTE Handoff

In releases prior to 20, QOS_CHANGE is reported as the value for Change-Condition AVP in the Service-Data-Container (SDC) of Rf accounting records (for accounting level SDF/SDF+accounting keys QCI) when eHRPD to LTE handoff occurs. Typically, the QOS_CHANGE should not be present as the PCRF does not enforce QoS via any QoS IE in eHRPD/CDMA RAT. In 20 and later releases, the SDC in the generated Rf record does not include QOS_CHANGE trigger during handoff from eHRPD to LTE.

QoS Change for Default Bearer

Releases prior to 20, in a multi-bearer call, when an update message (CCA-U or RAR) from PCRF changes the QoS (QCI/ARP) of default bearer and in the same message installs a predefined or dynamic rule on the newly updated default bearer, spurious Normal Release (NR) Service Data Volume (SDV) containers were added to Rf interim records for the dedicated bearers. In this scenario, the system used to send Normal Release buckets for the non-default bearers even if these bearers were not changed.

In release 20 and beyond, for a change in the QoS of default bearer, NR SDV containers will not be seen unless the corresponding bearer is torn down. Only QoS change containers are closed/released for the bearer that underwent QoS Change, i.e. the default bearer.

Diameter Rf Duplicate Record Generation

This section describes the overview and implementation of Rf Duplicate Record Generation feature.

This section discusses the following topics for this feature:

- [Feature Description, on page 720](#)
- [Configuring Rf Duplicate Record Generation, on page 721](#)
- [Monitoring and Troubleshooting the Rf Duplicate Record Generation, on page 723](#)

Feature Description

This feature is introduced to support creation and communication of duplicate Rf records to secondary AAA group servers configured for the Rf interface.

To achieve this functionality, the following configurations must be enabled –

- **aaa group** CLI command under APN to configure a maximum of 2 AAA groups - primary and secondary AAA groups, or two different endpoints for Rf Diameter accounting servers
- **diameter accounting duplicate-record** under AAA group to allow Rf duplicate record creation

The **diameter accounting duplicate-record** is a new CLI command introduced in this release for duplicating the Rf START, INTERIM and STOP accounting records.



Important

This is a license-controlled CLI command. For more information, contact your Cisco account representative.

In releases prior to 21, gateway allows only one AAA group configuration per APN for Rf accounting. The AAA group is configured to load balance across multiple servers to pass the Rf traffic and also expect an accounting answer. Note that the secondary AAA group configuration is allowed currently but is restricted to only RADIUS accounting.

In release 21 and beyond, the gateway is provided with the ability to configure a secondary AAA group per APN for the Rf interface, and send the duplicate Diameter Rf accounting records to the secondary AAA group servers. The secondary AAA group is used for non-billing purposes only.



Important

The failed duplicate records will neither be written to HDD nor added to the archival list.

There is no change in the current behavior with the primary AAA group messages. The primary AAA group is independent of the secondary AAA group, and it has multiple Rf servers configured. When the Rf servers do not respond even after multiple retries as per the applicable configuration, the Rf records are archived and stored in HDD. This behavior continues as is irrespective of the configuration of secondary aaa-group.

Secondary aaa group has a very similar configuration as the primary aaa group except that the new CLI command **diameter accounting duplicate-record** is additionally included to configure the secondary aaa-group. It is also important to note that different Diameter endpoints and a separate set of Rf servers should be provisioned for both primary and secondary AAA groups.

If all the configured servers are down, the request message will be discarded without writing it in HDD or archiving at aaamgr.

The original and duplicate Rf messages use two different aaa-groups and two different Diameter endpoints. Hence, the values for Session-ID AVP will be different. Based on the configuration of primary and secondary endpoints the values for Origin-Host, Origin-Realm, Destination-Realm, and Destination-Host AVPs may be different. Also based on the configuration under policy accounting for inclusion of virtual/gn apn name for secondary group Called-Station-ID AVP might change. All other AVPs will have the same values as with the primary aaa group Rf message.

Also, note that the values such as Acct-Interim-Interval (AII) interval received in ACA from secondary group of AAA servers will be ignored.

Relationships to Other Features

This feature can be used in conjunction with Virtual APN Truncation feature to achieve the desired results.

The Virtual APN Truncation feature is new in release 21. For more information on this feature, see the administration guide for the product you are deploying.

Limitations

The following are the limitations of this feature:

- Only one secondary AAA group can be configured per APN.
- If all the Rf peers under secondary aaa group are down and duplicate Start Record is not sent, then the duplicate Interim and Stop records will also not be sent to any of the secondary aaa group servers even though they arrived later. However if the servers are up and duplicate Start record was sent but the server did not respond, duplicate Start will be dropped after all the retries. In this case, the duplicate Interim and Stop records may be sent out to the server.
- In cases when duplicate Start record was sent, but during duplicate Interim/Stop record generation peers were not responding/down, after all retries duplicate Interim and Stop records will be dropped and will not be written to HDD.
- Minimal impact to memory and CPU is expected due to the duplicate record generation for every primary Rf record.

Configuring Rf Duplicate Record Generation

The following section provides the configuration commands to enable the Rf duplicate record generation.

Configuring Secondary AAA Group

Use the following configuration commands to configure the secondary AAA group for receiving the duplicate Rf records.

```
configure
  context context_name
    apn apn_name
      aaa group group_name
      aaa secondary-group group_name
    exit
```

Notes:

- **aaa group *group_name***: Specifies the AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.
- **secondary group *group_name***: Specifies the secondary AAA server group for the APN. *group_name* must be an alphanumeric string of 1 through 63 characters.

Configuring Duplication of Rf Records

Use the following configuration commands to configure the system to create a secondary feed of Rf records and send them to the secondary AAA group.

```
configure
  context context_name
    aaa group group_name
      diameter accounting duplicate-record
    exit
```

Notes:

- **duplicate-record**: Sends duplicate Rf records to configured secondary AAA group. This keyword is license dependent. For more information, contact your Cisco account representative.
- The default configuration is **no diameter accounting duplicate-record**. By default, this feature is disabled.
- The secondary aaa group must be configured under APN configuration mode before enabling the **diameter accounting duplicate-record** CLI command.

Verifying the Rf Duplicate Record Generation Configuration

Use the following commands to verify the configuration status of this feature.

```
show configuration
```

```
show aaa group all
```

- or -

```
show aaa group group_name
```

group_name must be the name of the AAA group specified during the configuration.

This command displays all the configurations that are enabled within the specified AAA group.

The following is a sample configuration of this feature.

```
configure
  context source
    apn domainname.com
      associate accounting-policy policy_accounting_name
      aaa group group1
        aaa secondary-group group2
      exit
    aaa group group1
      diameter accounting dictionary aaa-custom4
      diameter accounting endpoint rf_endpoint1
      diameter accounting server rf_server1 priority 1
      diameter accounting server rf_server2 priority 2
    exit
    aaa group group2
      diameter accounting dictionary aaa-custom4
      diameter accounting endpoint rf_endpoint2
      diameter accounting duplicate-record
      diameter accounting server rf_server3 priority 3
      diameter accounting server rf_server4 priority 4
    exit
```

```

diameter endpoint rf-endpoint1
  use-proxy
  origin host rf-endpoint1.carrier.com address 192.50.50.3
  no watchdog-timeout
  response-timeout 20
  connection retry-timeout 5
  peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
  peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
  exit
diameter endpoint rf-endpoint2
  use-proxy
  origin host rf-endpoint2.carrier.com address 192.50.50.2
  no watchdog-timeout
  response-timeout 20
  connection retry-timeout 5
  peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
  peer rf_server4 realm domainname.com address 192.50.50.5 port 4893

```

end

Notes:

- The **diameter accounting duplicate-record** CLI is license specific. So, the corresponding license must be enabled for the CLI command to be configured.
- Both primary and secondary aaa groups are preferred to have different accounting endpoint names.

Monitoring and Troubleshooting the Rf Duplicate Record Generation

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration** or **show aaa group all** CLI command. If not enabled, configure the diameter accounting duplicate-record CLI command and check if it works.
- Collect the output of **show diameter aaa statistics** command and analyze the debug statistics. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.

show diameter aaa-statistics

The following statistics are added to the output of this show command for duplicate Rf records which were dropped because of the failure in sending the Accounting records instead of adding them to HDD or archival list.

- Duplicate Accounting Records Stats
 - ACR-Start Dropped
 - ACR-Interim Dropped
 - ACR-Stop Dropped

These statistics are maintained per aaamgr instance level. For descriptions of these statistics, see the *Statistics and Counters Reference* guide.

These statistics can also be collected per group basis/server basis for duplicate records i.e. through **show diameter aaa-statistics group** <group_name> and **show diameter aaa-statistics server** <server_name> CLI commands.

Truncation of Virtual APN for Rf Records

This feature enables the truncation of Virtual APN (VAPN) returned by S6b server to be sent to Gx, Gy and Rf interfaces.

Feature Description

Currently there is no way to quickly turn on the Rf accounting to the Data Streaming Service (DSS) server per Virtual APN (S6b-VAPN) without reaching all nodes in the network and provision the Virtual APN on each of them. This feature is implemented to truncate the virtual APN name returned by S6b server with the configured standard delimiters. In this way a single configuration per node can be utilized for all enterprises based on a virtual APN. This approach will significantly reduce the size and time to provision new enterprises with the requested feature.

To achieve this functionality, a configuration is added per APN to enable truncation of S6b-VAPN and also to configure the delimiter(s) where the APN name is to be truncated. Standard delimiters like (.) and (-) are used since APN name supports only these two characters apart from the alphanumeric ones.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

AAA manager performs the truncation of the Virtual APN name based on the APN configuration and provides the correct APN profile for the truncated APN name. If the truncation is successful, the full virtual APN name will be sent to Gx, Gy and Rf interfaces.

Accounting records are required to support real-time usage notification and device management functionality. So, the **apn-name-to-be-included** CLI command is extended to enable actual APN (Gn-APN) or virtual APN (S6b returned virtual APN) name to be included in Called-Station-ID AVP in the secondary Rf accounting records (secondary server group) under policy accounting configuration. Currently, policy accounting configuration supports sending the Gn-APN/S6b-VAPN in Called-Station-ID for primary Rf server. With this CLI command, this functionality is extended for the secondary Rf server.

A new AAA attribute "Secondary-Called-Station-ID" is added to support sending Gn/Virtual APN name in the Called-Station-ID AVP for duplicate Rf records sent to secondary group Rf server.

Configuring Virtual APN Truncation for Rf Records

The following section provides the configuration commands to enable the Virtual APN Truncation feature for Rf records.

Configuring Gn-APN/VAPN for Rf Accounting

Use the following configuration commands to configure the actual APN or Virtual APN (VAPN) for Rf accounting.

```
configure
  context context_name
```



```

policy accounting policy_name
  apn-name-to-be-included { gn | virtual } [ secondary-group { gn | virtual } ]
end

```

Notes:

- **apn-name-to-be-included:** Configures the APN name to be included in the Rf messages for primary server group.
- **secondary-group { gn | virtual }:** Configures the APN name to be included in the Rf messages for secondary server group.
- **gn:** Configures the Gn APN name to be included in the Rf messages.
- **virtual:** Configures the virtual APN name to be included in the Rf messages.
- By default, the apn name to be included in Called-Station-ID AVP is Gn-APN for both primary and secondary Rf server groups.
- If the secondary group configuration is not available, the default behavior is to have Gn APN for secondary Rf group duplicate records.

Configuring Truncation of Virtual APN

Use the following configuration commands to configure the gateway to truncate the APN name returned from S6b interface.

```

configure
context context_name
  apn apn_name
    virtual-apn { gcdr apn-name-to-be-included { gn | virtual } | truncate-s6b-vapn delimiter {
dot [ hyphen ] | hyphen [ dot ] } }
    end
end

```

Notes:

- For information on the existing keywords, see the *Command Line Interface Reference* guide.
- **truncate-s6b-vapn:** Allows truncation of virtual APN received from S6b at the configured delimiter character.
- **delimiter { dot [hyphen] | hyphen [dot] }:** Configures the delimiter for truncation of virtual APN received from S6b. If the CLI command is configured, the S6b returned virtual APN will be truncated at the configured delimiter.
 - **dot:** Configures the delimiter to dot (.) for truncation of S6b-VAPN
 - **hyphen:** Configures the delimiter to hyphen (-) for truncation of S6b-VAPN
- Both dot and hyphen delimiters can be configured in the same line or a new line.
- **no virtual-apn truncate-s6b-vapn:** Disables the truncation of virtual APN name. If both delimiters should be disabled at once, use the **no virtual-apn truncate-s6b-vapn** CLI command.
If a particular delimiter needs to be disabled, it should be done explicitly. For example, if the dot delimiter should be disabled, use the **no virtual-apn truncate-s6b-vapn delimiter dot** CLI command.
- By default this feature will be disabled and no delimiter will be configured.
- This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message.

- If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

Verifying the Virtual APN Truncation Configuration

Use the following command to verify the configuration status of this feature.

show configuration apn *apn_name*

apn_name must be the name of the APN specified during the feature configuration.

This command displays all the configurations that are enabled within the specified APN name. The following is a sample output of this show command.

```
[local]st40# show configuration apn intershat
configure
  context ingress
    apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      virtual-apn truncate-s6b-vapn delimiter hyphen
    end
```

Monitoring and Troubleshooting the Virtual APN Truncation

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show configuration apn *apn_name*** CLI command. If not enabled, configure the **virtual-apn truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] }** CLI command and check if it works.
- Collect the output of **show apn statistics** CLI command and analyze the debug statistics. For further assistance, contact Cisco account representative.



Important

For P-GW, GGSN and SAEGW services, if the truncation of S6b returned virtual APN name fails and the virtual APN name is not configured, the call will be rejected with 'unknown-apn-name' cause.

show apn statistics

This show command uses the existing APN statistics to populate the truncated virtual APN name, if this feature is enabled.

show subscribers ggsn-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a'.

- S6b Returned Virtual APN

show subscribers pgw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a'.

- S6b Returned Virtual APN

show subscribers saegw-only full all

The following field added newly to the output of this show command displays the S6b returned full virtual APN name, if this feature is enabled. Otherwise, it displays 'n/a'.

- S6b Returned Virtual APN

How it Works

This section describes how offline charging for subscribers works with Rf interface support in GPRS/eHRPD/LTE/IMS networks.

The following figure and table explain the transactions that are required on the Diameter Rf interface in order to perform event based charging. The operation may alternatively be carried out prior to, concurrently with or after service/content delivery.

Figure 98: Rf Call Flow for Event Based Charging

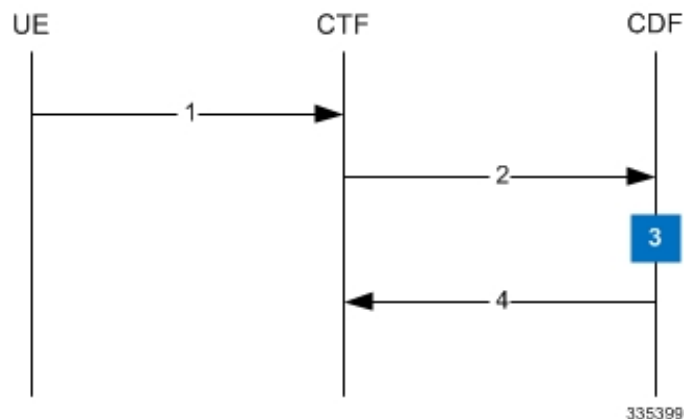


Table 58: Rf Call Flow Description for Event Based Charging

Step	Description
1	The network element (CTF) receives indication that service has been used/delivered.
2	The CTF (acting as Diameter client) sends Accounting-Request (ACR) with Accounting-Record-Type AVP set to EVENT_RECORD to indicate service specific information to the CDF (acting as Diameter server).

Step	Description
3	The CDF receives the relevant service charging parameters and processes accounting request.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type AVP set to EVENT_RECORD to the CTF in order to inform that charging information was received.

The following figure and table explain the simple Rf call flow for session based charging.

Figure 99: Rf Call Flow for Session Based Charging

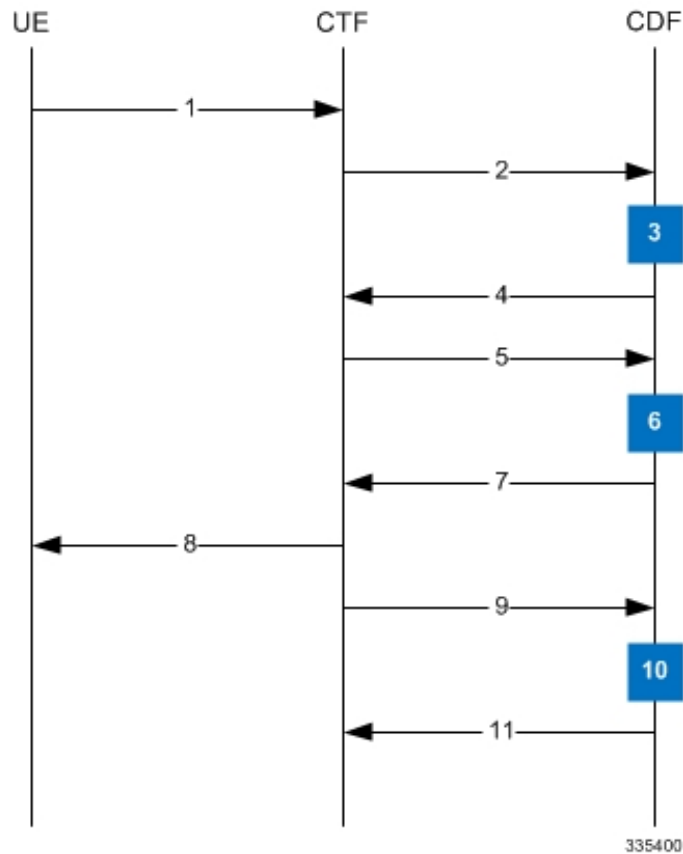


Table 59: Rf Call Flow Description for Session Based Charging

Step	Description
1	The CTF receives a service request. The service request may be initiated either by the user or the other network element.
2	In order to start accounting session, the CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to START_RECORD to the CDF.

Step	Description
3	The session is initiated and the CDF opens a CDR for the current session.
4	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to START_RECORD to the CTF and possibly Acct-Interim-Interval AVP (AII) set to non-zero value indicating the desired intermediate charging interval.
5	When either AII elapses or charging condition changes are recognized at CTF, the CTF sends an Accounting-Request (ACR) with Accounting-Record-Type AVP set to INTERIM_RECORD to the CDF.
6	The CDF updates the CDR in question.
7	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to INTERIM_RECORD to the CTF.
8	The service is terminated.
9	The CTF sends a Accounting-Request (ACR) with Accounting-Record-Type AVP set to STOP_RECORD to the CDF.
10	The CDF updates the CDR accordingly and closes the CDR.
11	The CDF returns Accounting-Answer (ACA) message with Accounting-Record-Type set to STOP_RECORD to the CTF.

Configuring Rf Interface Support

To configure Rf interface support:

- 1 Configure the core network service as described in this Administration Guide.
- 2 Enable Active Charging Service (ACS) and create ACS as described in the *Enhanced Charging Services Administration Guide*.



Important

The procedures in this section assume that you have installed and configured your chassis including the ECS installation and configuration as described in the *Enhanced Charging Services Administration Guide*.

- 3 Enable Rf accounting in ACS as described in [Enabling Rf Interface in Active Charging Service](#), on page 730.
- 4 Configure Rf interface support as described in the relevant sections:
 - [Configuring GGSN / P-GW Rf Interface Support](#), on page 730
 - [Configuring P-CSCF/S-CSCF Rf Interface Support](#), on page 739

**Important**

In StarOS versions 19 and later, the Rf interface is not supported on the S-GW.

- 5 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

**Important**

Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Enabling Rf Interface in Active Charging Service

To enable the billing record generation and Rf accounting, use the following configuration:

```
configure
active-charging service <service_name>
rulebase <rulebase_name>
  billing-records rf
  active-charging rf { rating-group-override | service-id-override }
end
```

Notes:

- Prior to creating the Active Charging Service (ACS), the **require active-charging** command should be configured to enable ACS functionality.
- The **billing-records rf** command configures Rf record type of billing to be performed for subscriber sessions. Rf accounting is applicable only for dynamic and predefined ACS rules.

For more information on the rules and its configuration, refer to the *ACS Charging Action Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

- The **active-charging rf** command is used to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

For more information on this command, refer to the *ACS Rulebase Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Configuring GGSN / P-GW Rf Interface Support

To configure the standard Rf interface support for GGSN/P-GW, use the following configuration:

```
configure
context <context_name>
  apn <apn_name>
  associate accounting-policy <policy_name>
```

```

exit
policy accounting <policy_name>
  accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout
  | location-change | rai-change | tai-change } action { interim | stop-start }
  accounting-keys qci
  accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
  cc profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets
  { uplink octets } | total octets | uplink octets { downlink octets } } | serving-nodes num | tariff time1 min
  hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets } | total octets | uplink
  octets { downlink octets } } }
  max-containers { containers | fill-buffer }
end

```

Notes:

- The policy can be configured in any context.
- For information on configuring accounting levels/policies/modes/event triggers, refer to the *Accounting Policy Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- Depending on the triggers configured, the containers will either be cached or released. In the case of GGSN/P-GW, the containers will be cached when the event trigger is one of the following:

- QOS_CHANGE
- FLOW_INFORMATION_CHANGE
- LOCATION_CHANGE
- SERVING_NODE_CHANGE
- SERVICE_IDLE
- SERVICE_DATA_VOLUME_LIMIT
- SERVICE_DATA_TIME_LIMIT
- IP_FLOW_TERMINATION
- TARIFF_CHANGE

If the event trigger is one of the following, the containers will be released:

- VOLUME_LIMIT
- TIME_LIMIT
- RAT_CHANGE
- TIMEZONE_CHANGE
- PLMN_CHANGE



Important

Currently, SDF and flow level accounting are supported in P-GW.

The following assumptions guide the behavior of P-GW, GGSN and CCF for Change-Condition triggers:

- Data in the ACR messages due to change conditions contain the snapshot of all data that is applicable to the interval of the flow/session from the previous ACR message. This includes all data that is already sent and has not changed (e.g. SGSN-Address).
- All information that is in a PDN session/flow up to the point of the Change-Condition trigger is captured (snapshot) in the ACR-Interim messages. Information about the target Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change/etc will be in subsequent Rf messages.

Table 60: P-GW/GGSN and CCF Behavior for Change-Condition in ACR-Stop and ACR-Interim for LTE/e-HRPD/GGSN

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Stop	Normal Release	YES	NO	YES	Normal Release	Normal Release	When PDN/IP session is closed, C-C in both level will have Normal Release.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Normal Release	YES	NO	NO	N/A	Normal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
Stop	Abnormal Release	YES	NO	YES	Abnormal Release	Abnormal Release	When PDN/IP session is closed, C-C in both level will have Abnormal Release.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Abnormal Release	YES	NO	NO	N/A	Abnormal Release	Flow is closed, SDC CC is populated and closed container is added to record. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	QoS-Change	YES	NO	NO	N/A	QoS-Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
Interim	Volume Limit	YES	YES	NO	Volume Limit	Volume Limit	For PDN/IP Session Volume Limit. The Volume Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry this charging profile that will be passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Time Limit	YES	YES	NO	Time Limit	Time Limit	For PDN/IP Session Time Limit. The Time Limit is configured as part of the Charging profile and the Charging-Characteristics AVP will carry this charging profile that will be passed on from the HSS/AAA to P-GW/GGSN through various interfaces. The charging profile will be provisioned in the HSS.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Serving Node Change	YES	NO	NO	N/A	Serving Node Change	The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
Interim	Serving Node PLMN Change	YES	YES	NO	Serving Node PLMN Change	Serving Node PLMN Change	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	User Location Change	YES	NO	NO	N/A	User Location Change	This is BSID Change in eHRPD. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
Interim	RAT Change	YES	YES	NO	RAT Change	RAT Change	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	UE Timezone Change	YES	YES	NO	UE Timezone change	UE Timezone change	This is not applicable for eHRPD.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Tariff Time Change	YES	NO	NO	N/A	Tariff Time Change	Triggered when Tariff Time changes. Tariff Time Change requires an online charging side change. The implementation of this Change Condition is dependent on implementation of Online Charging update.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Idled Out	YES	NO	NO	N/A	Service Idled Out	Flow Idled out. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Volume Limit	YES	NO	NO	N/A	Service Data Volume Limit	Volume Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
None (as this change condition is a counter for the Max Number of Changes in Charging Conditions).	Service Data Time Limit	YES	NO	NO	N/A	Service Data Time Limit	Time Limit reached for a specific flow. The container for this change condition will be cached by the P-GW/GGSN and the container will be in a ACR Interim/Stop sent for partial record (Interim), final Record (Stop) or All trigger (Interim) trigger.

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
Interim	Max Number of Changes in Charging Conditions	YES	YES	NO	YES	YES, Will include SDC that corresponds to the CCs that occurred (Normal Release of Flow, Abnormal Release of Flow, QoS-Change, Serving Node Change, User Location Change, Tariff Time Change, Service Idled Out, Service Data Volume Limit, Service Data Time Limit)	

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							<p>This ACR[Interim] is triggered at the instant when the Max Number of changes in charging conditions takes place. Max Change Condition is applicable for QoS-Change, Service-Idled Out, ULI change, Flow Normal Release, Flow Abnormal Release, Service Data Volume Limit, Service Data Time Limit, All Timer ACR Interim and Service Node Change CC only. The Max Number of Changes in Charging Conditions is set at 10. Example assuming 1 flow in the PDN Session: [1] Max Number of Changes in Charging Conditions set at P-GW/GGSN = 2. [2] Change Condition 1 takes place. No ACR Interim is sent. P-GW/GGSN stores the SDC. [3] Change Condition 2 takes place. An ACR Interim is sent. Now Max Number of Changes in Charging conditions is populated in the PS-Information 2 Service-Data-Containers (1 for each change condition) are</p>

ACR Message	Change-Condition Value	CCF Response to Change-Condition Value			CC Level Population		Comments
		Addition of Container	Partial FDR	Final FDR	PS-Information Level	SDC Level	
							populated in the ACR Interim. [4] CCF creates the partial record.
Stop	Management Intervention	YES	NO	YES	YES	YES	Management intervention will close the PDN session from P-GW/GGSN.
Interim	-	YES	NO	NO	N/A	N/A	This is included here to indicate that an ACR[Interim] due to AII timer will contain one or more populated SDC/s for a/all flow/s, but Change-Condition AVP will NOT be populated.

Configuring P-CSCF/S-CSCF Rf Interface Support

To configure P-CSCF/S-CSCF Rf interface support, use the following configuration:

```

configure
context vpn
aaa group default
diameter authentication dictionary aaa-custom8
diameter accounting dictionary aaa-custom2
diameter accounting endpoint <endpoint_name>
diameter accounting server <server_name> priority <priority>
exit
diameter endpoint <endpoint_name>
origin realm <realm_name>
use-proxy
origin host <host_name> address <ip_address>
peer <peer_name> address <ip_address>
exit
end

```

Notes:

- For information on commands used in the basic configuration for Rf support, refer to the *Command Line Interface Reference*.

Gathering Statistics

This section explains how to gather Rf and related statistics and configuration information.

In the following table, the first column lists what statistics to gather, and the second column lists the action to perform.

Statistics/Information	Action to perform
Complete statistics for Diameter Rf accounting sessions	show diameter aaa-statistics

The following is a sample output of the **show diameter aaa-statistics** command:

Authentication Servers Summary

```

-----
Message Stats :
  Total MA Requests:          0      Total MA Answers:          0
  MAR - Retries:              0      MAA Timeouts:              0
  MAA - Dropped:              0
  Total SA Requests:          0      Total SA Answers:          0
  SAR - Retries:              0      SAA Timeouts:              0
  SAA - Dropped:              0
  Total UA Requests:          0      Total UA Answers:          0
  UAR - Retries:              0      UAA Timeouts:              0
  UAA - Dropped:              0
  Total LI Requests:          0      Total LI Answers:          0
  LIR - Retries:              0      LIA Timeouts:              0
  LIA - Dropped:              0
  Total RT Requests:          0      Total RT Answers:          0
  RTR - Rejected:             0
  Total PP Requests:          0      Total PP Answers:          0
  PPR - Rejected:             0
  Total DE Requests:          0      Total DE Answers:          0
  DEA - Accept:               0      DEA - Reject:              0
  DER - Retries:              0      DEA Timeouts:              0
  DEA - Dropped:              0
  Total AA Requests:          0      Total AA Answers:          0
  AAR - Retries:              0      AAA Timeouts:              0
  AAA - Dropped:              0
  ASR:                        0      ASA:                        0
  RAR:                        0      RAA:                        0
  STR:                        0      STA:                        0
  STR - Retries:              0

Message Error Stats:
  Diameter Protocol Errs:      0      Bad Answers:                0
  Unknown Session Reqs:        0      Bad Requests:                0
  Request Timeouts:            0      Parse Errors:                0
  Request Retries:             0

Session Stats:
  Total Sessions:              0      Freed Sessions:              0
  Session Timeouts:            0      Active Sessions:             0

STR Termination Cause Stats:
  Diameter Logout:             0      Service Not Provided:        0
  Bad Answer:                  0      Administrative:              0
  Link Broken:                  0      Auth Expired:                0
  User Moved:                  0      Session Timeout:             0
  User Request:                 0      Lost Carrier:                 0
  Lost Service:                 0      Idle Timeout:                 0
  NAS Session Timeout:          0      Admin Reset:                  0
  Admin Reboot:                 0      Port Error:                   0
  NAS Error:                    0      NAS Request:                  0
  NAS Reboot:                   0      Port Unneeded:                0
  Port Preempted:               0      Port Suspended:               0
  Service Unavailable:          0      Callback:                     0

```


User Error:	0	Host Request:	0
Accounting Servers Summary			

Message Stats :			
Total AC Requests:	0	Total AC Answers:	0
ACR-Start:	0	ACA-Start:	0
ACR-Start Retries :	0	ACA-Start Timeouts:	0
ACR-Interim:	0	ACA-Interim:	0
ACR-Interim Retries :	0	ACA-Interim Timeouts:	0
ACR-Event:	0	ACA-Event:	0
ACR-Stop :	0	ACA-Stop:	0
ACR-Stop Retries :	0	ACA-Stop Timeouts:	0
ACA-Dropped :	0		
AC Message Error Stats:			
Diameter Protocol Errs:	0	Bad Answers:	0
Unknown Session Reqs:	0	Bad Requests:	0
Request Timeouts:	0	Parse Errors:	0
Request Retries:	0		



Subscriber Overcharging Protection

Subscriber Overcharging Protection is a proprietary, enhanced feature that prevents subscribers in UMTS networks from being overcharged when a loss of radio coverage (LORC) occurs. This chapter indicates how the feature is implemented on various systems and provides feature configuration procedures. Products supporting subscriber overcharging protection include Cisco's Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN).

The individual product administration guides provide examples and procedures for configuration of basic services. Before using the procedures in this chapter, we recommend that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective guide.



Important

Subscriber Overcharging Protection is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

This chapter covers the following topics in support of the Subscriber Overcharging Protection feature:

- [Feature Overview, page 743](#)
- [Overcharging Protection - GGSN Configuration, page 744](#)
- [Overcharging Protection - SGSN Configuration, page 746](#)

Feature Overview

Subscriber Overcharging Protection enables the SGSN to avoid overcharging the subscriber if/when a loss of radio coverage (LORC) occurs.

When a mobile is streaming or downloading files from external sources (for example, via a background or interactive traffic class) and the mobile goes out of radio coverage, the GGSN is unaware of such loss of connectivity and continues to forward the downlink packets to the SGSN.

Previously, upon loss of radio coverage (LORC), the SGSN did not perform the UPC procedure to set QoS to 0kbps, as it does when the traffic class is either streaming or conversational. Therefore, when the SGSN did a Paging Request, if the mobile did not respond the SGSN would simply drop the packets without notifying

the GGSN; the G-CDR would have increased counts but the S-CDR would not, causing overcharges when operators charged the subscribers based on the G-CDR.

Now operators can accommodate this situation, they can configure the SGSN to set QoS to 0kbps, or to a negotiated value, upon detecting the loss of radio coverage. The overcharging protection feature relies upon the SGSN adding a proprietary private extension to GTP LORC Intimation IE to messages. This LORC Intimation IE is included in UPCQ, DPCQ, DPCR, and SGSN Context Response GTP messages. One of the functions of these messages is to notify the GGSN to prevent overcharging.

The GGSN becomes aware of the LORC status by recognizing the message from the SGSN and discards the downlink packets if LORC status indicates loss of radio coverage or stops discarding downlink packets if LORC status indicates gain of radio coverage for the UE.

The following table summarizes the SGSN's actions when radio coverage is lost or regained and LORC overcharging protection is enabled.

Table 61: LORC Conditions and Overcharging Protection

Condition	Triggered by	SGSN Action	LORC Intimation IE - private extension payload
Loss of radio coverage (LORC)	RNC sends Iu release request with cause code matching configured value	Send UPCQ to GGSN Start counting unsent packets/bytes Stop forwarding packets in downlink direction	No payload
Mobile regains coverage in same SGSN area	MS/SGSN	Send UPCQ to GGSN Stop counting unsent packets/bytes Stop discarding downlink packets	New loss-of-radio-coverage state and unsent packet/byte counts
Mobile regains coverage in different SGSN area	MS/SGSN	Send SGSN Context Response message to new SGSN Stop counting unsent packets/bytes	Unsent packet/byte counts
PDP deactivated during LORC	MS/SGSN	Send DPCQ to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts
PDP deactivated during LORC	GGSN	Send DPCR to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts

Overcharging Protection - GGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the GGSN to support subscriber overcharging protection.

**Important**

This section provides the minimum instruction set to configure the GGSN to avoid the overcharging due to loss of radio coverage in UMTS network. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - SGSN Configuration* also in this chapter. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in *System Administration Guide* and the *Gateway GPRS Support Node Administration Guide*.

To configure the system to support overcharging protection on LORC in the GGSN service:

-
- Step 1** Configure the GTP-C private extension in a GGSN service by applying the example configurations presented in the *GTP-C Private Extension Configuration* section below.
- Step 2** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 3** Verify configuration of overcharging protection on LORC related parameters by applying the commands provided in the *Verifying Your GGSN Configuration* section in this chapter.
-

GTP-C Private Extension Configuration

This section provides the configuration example to configure the GTP-C private extensions for GGSN service:

configure

```
context vpn_context_name
  ggsn-service ggsn_svc_name
    gtpc private-extension loss-of-radio-coverage
  end
```

Notes:

- *vpn_context_name* is the name of the system context where specific GGSN service is configured. For more information, refer *Gateway GPRS Support Node Administration Guide*.
- *ggsn_svc_name* is the name of the GGSN service where you want to enable the overcharging protection for subscribers due to LORC.

Verifying Your GGSN Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file (as described in the *Verifying and Saving Your Configuration* chapter in this book) and how to retrieve errors and warnings within an active configuration for a service.

**Important**

All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the overcharging protection support configuration.

Step 1

Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

show ggsn-service name *ggsn_svc_name*

The output of this command displays the configuration for overcharging protection configured in the GGSN service *ggsn_svc_name*.

```
Service name:          ggsn_svc1
Context:              service
Accounting Context Name: service
Bind:                 Done
Local IP Address:     192.169.1.1      Local IP Port:    2123
...
...
GTP Private Extensions:
  Preservation Mode
  LORC State
```

Step 2

Verify that GTP-C private extension is configured properly for GGSN subscribers by entering the following command in Exec Mode:

show subscribers ggsn-only full

The output of this command displays the LORC state information and number of out packets dropped due to LORC.

Overcharging Protection - SGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the SGSN to support subscriber overcharging protection.

**Important**

This section provides a minimum instruction set to configure the SGSN to implement this feature. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - GGSN Configuration* also in this chapter.

Command details can be found in the *Command Line Interface Reference*.

These instructions assume that you have already completed:

- the system-level configuration as described in the *System Administration Guide*,
- the SGSN service configuration as described in the *Serving GPRS Support Node Administration Guide*, and
- the configuration of an APN profile as described in the *Operator Policy* chapter in this guide.

To configure the SGSN to support subscriber overcharging protection:

Step 1

Configure the private extension IE with LORC in an APN profile by applying the example configurations presented in the *Private Extension IE Configuration* section.

Note An APN profile is a component of the Operator Policy feature implementation. To implement this feature, an APN profile must be created and *associated* with an operator policy. For details, refer to the *Operator Policy* chapter in this book.

- Step 2** Configure the RANAP cause that should trigger this UPCQ message by applying the example configurations presented in the *RANAP Cause Trigger Configuration* section.
- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.
- Step 4** Verify the SGSN portion of the configuration for overcharging protection on LORC related parameters by applying the commands provided in the *Verifying the Feature Configuration* section.
-

Private Extension IE Configuration

This section provides the configuration example to enable adding the private extension IE that will be included in the messages sent by the SGSN when a loss of radio coverage occurs in the UMTS network:

configure

```
apn-profile apn_profile_name
  gtp private-extension loss-of-radio-coverage send-to-ggsn
end
```

Note:

- *apn_profile_name* is the name of a previously configured APN profile. For more information, refer to the *Operator Policy* chapter, also in this book.

RANAP Cause Trigger Configuration

This section provides the configuration example to enable the RANAP cause trigger and define the trigger message value:

configure

```
context context_name
  iups-service iups_service_name
    loss-of-radio-coverage ranap-cause cause
end
```

Notes:

- *context_name* is the name of the previously configured context in which the IuPS service has been configured.
- *cause* is an integer from 1 to 512 (the range of reasons is a part of the set defined by 3GPP TS 25.413) that allows configuration of the RANAP Iu release cause code to be included in messages. Default is 46 (MS/UE radio connection lost).

Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a *.cfg* file as described in the *Verifying and Saving Your Configuration* chapter elsewhere in this guide.



Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the overcharging protection support configuration.

Step 1

Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

show apn-profile full name *apn_profile_name*

The output of this command displays the entire configuration for the APN profile configuration. Only the portion related to overcharging protection configuration in the SGSN is displayed below. Note that the profile name is an example:

```
APN Profile name:           : apnprofile1
Resolution Priority:        : dns-fallback
...
...
Sending Private Extension Loss of Radio Coverage IE
    To GGSN                 : Enabled
    To SGSN                 : Enabled
```

Step 2

Verify the RANAP Iu release cause configuration by entering the following command in the Exec Mode:

show iups-service name *iups_service_name*

The output of this command displays the entire configuration for the IuPS service configuration. Only the portion related to overcharging protection configuration (at the end of the display) is displayed below. Note that the IuPS service name is an example:

```
Service name                : iups1
Service-ID                  : 1
...
...
Loss of Radio Coverage
Detection Cause in Iu Release : 46
```



Traffic Policing and Shaping

This chapter describes the support of per subscriber Traffic Policing and Shaping feature on Cisco's Chassis and explains the commands and RADIUS attributes that are used to implement this feature. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

Traffic Policing and Shaping is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The following topics are included:

- [Overview, page 749](#)
- [Traffic Policing Configuration, page 750](#)
- [Traffic Shaping Configuration, page 753](#)
- [RADIUS Attributes, page 756](#)

Overview

This section describes the traffic policing and shaping feature for individual subscriber. This feature is comprised of two functions:

- Traffic Policing
- Traffic Shaping

Traffic Policing

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers and/or APN of a particular traffic class in 3GPP/3GPP2 service.

Bandwidth enforcement is configured and enforced independently on the downlink and the uplink directions.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the Traffic-Policing feature. The algorithm used measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.
- **Burst-size:** The maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

The system can be configured to take any of the following actions on packets that are determined to be in excess or in violation:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS bit is set to "0", thus downgrading it to Best Effort, prior to passing the packet. Note that if the packet's ToS bit was already set to "0", this action is equivalent to "Transmit".

Traffic Shaping

Traffic Shaping is a rate limiting method similar to the Traffic Policing, but provides a buffer facility for packets exceeded the configured limit. Once the packet exceeds the data-rate, the packet queued inside the buffer to be delivered at a later time.

The bandwidth enforcement can be done in the downlink and the uplink direction independently. If there is no more buffer space available for subscriber data system can be configured to either drop the packets or kept for the next scheduled traffic session.



Important

Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

Traffic Policing Configuration

Traffic Policing is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.

**Important**

In 3GPP service attributes received from the RADIUS server supersede the settings in the APN.

**Important**

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring Subscribers for Traffic Policing

**Important**

Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Step 1

Configure local subscriber profiles on the system to support Traffic Policing by applying the following example configurations:

- a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
      qos traffic-police direction downlink
    end
```

- b) To apply the specified limits and actions to the uplink (data from the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
      qos traffic-police direction uplink
    end
```

Notes:

- There are numerous keyword options associated with the **qos traffic-police direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.

Note If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

Step 2

Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>
  show subscriber configuration username <user_name>
```

- Step 3** Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN for Traffic Policing in 3GPP Networks

This section provides information and instructions for configuring APN template's QoS profile in support of Traffic Policing.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the table below.

Table 62: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g. 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 8640000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

- Step 1** Set parameters by applying the following example configurations:

- a) To apply the specified limits and actions to the downlink (the Gn direction):

```
configure
  context <context_name>
    apn <apn_name>
      qos rate-limit downlink
    end
```

- b) To apply the specified limits and actions to the uplink (the Gi direction):

```
configure
  context <context_name>
    apn <apn_name>
      qos rate-limit uplink
    end
```

Notes:

- There are numerous keyword options associated with **qos rate-limit { downlink | uplink }** command.
- *Optionally*, configure the maximum number of PDP contexts that can be facilitated by the APN to limit the APN's bandwidth consumption by entering the following command in the configuration:
max-contents primary <number> total <total_number>
- Repeat as needed to configure additional Qos Traffic Policing profiles.

Important If a "subscribed" traffic class is received, the system changes the class to background and sets the following: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the background class. The received values are used for responses when traffic policing is disabled.

Step 2 Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Traffic Shaping Configuration

Traffic Shaping is configured on a per-subscriber basis. The subscribers can either be locally configured subscribers on the system or subscriber profiles configured on a remote RADIUS server.

In 3GPP service Traffic policing can be configured for subscribers through APN configuration as well.



Important

In 3GPP, service attributes received from the RADIUS server supersede the settings in the APN.



Important

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.



Important

Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

Configuring Subscribers for Traffic Shaping

This section provides information and instructions for configuring local subscriber profiles on the system to support Traffic Shaping.



Important

Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Step 1

Set parameters by applying the following example configurations:

- a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
      qos traffic-shape direction downlink
    end
```

- b) To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
      qos traffic-shape direction uplink
    end
```

Notes:

- There are numerous keyword options associated with **qos traffic-shape direction { downlink | uplink }** command.
- Repeat for each additional subscriber to be configured.

Important

If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos-copy** command in the Subscriber Configuration mode is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command (also in the Subscriber Configuration mode). Therefore, it is recommended that command not be used when specifying this option.

Step 2

Verify the subscriber profile configuration by applying the following example configuration:

```
context <context_name>
  show subscriber configuration username <user_name>
```

Step 3

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN for Traffic Shaping in 3GPP Networks

This section provides information and instructions for configuring APN template's QoS profile in support of Traffic Shaping.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that values for the committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the following table.

Table 63: Permitted Values for Committed and Peak Data Rates in GTP Messages 0

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g. 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 576,000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 8640000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

Step 1

Set parameters by applying the following example configurations.

- a) To apply the specified limits and actions to the downlink (data to the subscriber):

```
configure
  context <context_name>
    subscriber name <user_name>
    qos rate-limit downlink
  end
```

- b) To apply the specified limits and actions to the uplink (data to the subscriber):

```
configure
  context <context_name>
    apn <apn_name>
    qos rate-limit uplink
  end
```

Step 2

Verify that your APNs were configured properly by entering the following command:

```
show apn { all | name <apn_name> }
```

The output is a concise listing of configured APN parameter settings.

Step 3

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

RADIUS Attributes

Traffic Policing for CDMA Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for CDMA subscribers (PDSN, HA) configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 64: RADIUS Attributes Required for Traffic Policing Support for CDMA Subscribers

Attribute	Description
SN-QoS-Tp-Dnlk (or SN1-QoS-Tp-Dnlk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Dnlk-Committed-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink committed-data-rate in bps.
SN-Tp-Dnlk-Peak-Data-Rate (or SN1-Tp-Dnlk-Committed-Data-Rate)	Specifies the downlink peak-data-rate in bps.
SN-Tp-Dnlk-Burst-Size (or SN1-Tp-Dnlk-Burst-Size)	Specifies the downlink-burst-size in bytes. NOTE: It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Dnlk-Exceed-Action (or SN1-Tp-Dnlk-Exceed-Action)	Specifies the downlink exceed action to perform.
SN-Tp-Dnlk-Violate-Action (or SN1-Tp-Dnlk-Violate-Action)	Specifies the downlink violate action to perform.
SN-QoS-Tp-Uplk (or SN1-QoS-Tp-Uplk)	Enable/disable traffic policing in the downlink direction.
SN-Tp-Uplk-Committed-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink committed-data-rate in bps.
SN-Tp-Uplk-Peak-Data-Rate (or SN1-Tp-Uplk-Committed-Data-Rate)	Specifies the uplink peak-data-rate in bps.

Attribute	Description
SN-Tp-Uplk-Burst-Size (or SN1-Tp-Uplk-Burst-Size)	Specifies the uplink-burst-size in bytes. Note It is recommended that this parameter be configured to at least the greater of the following two values: 1) 3 times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.
SN-Tp-Uplk-Exceed-Action (or SN1-Tp-Uplk-Exceed-Action)	Specifies the uplink exceed action to perform.
SN-Tp-Uplk-Violate-Action (or SN1-Tp-Uplk-Violate-Action)	Specifies the uplink violate action to perform.

Traffic Policing for UMTS Subscribers

The RADIUS attributes listed in the following table are used to configure Traffic Policing for UMTS subscribers configured on remote RADIUS servers. More information on these attributes can be found in the *AAA Interface Administration and Reference*.

Table 65: RADIUS Attributes Required for Traffic Policing Support for UMTS Subscribers

Attribute	Description
SN-QoS-Conversation-Class (or SN1-QoS-Conversation-Class)	Specifies the QOS Conversation Traffic Class.
SN-QoS-Streaming-Class (or SN1-QoS-Streaming-Class)	Specifies the QOS Streaming Traffic Class.
SN-QoS-Interactive1-Class (or SN1-QoS-Interactive1-Class)	Specifies the QOS Interactive Traffic Class.
SN-QoS-Interactive2-Class (or SN1-QoS-Interactive2-Class)	Specifies the QOS Interactive2 Traffic Class.
SN-QoS-Interactive3-Class (or SN1-QoS-Interactive3-Class)	Specifies the QOS Interactive3 Traffic Class.
SN-QoS-Background-Class (or SN1-QoS-Background-Class)	Specifies the QOS Background Traffic Class.

Attribute	Description
SN-QoS-Traffic-Policy (or SN1-QoS-Traffic-Policy)	<p>This compound attribute simplifies sending QoS values for Traffic Class (the above attributes), Direction, Burst-Size, Committed-Data-Rate, Peak-Data-Rate, Exceed-Action, and Violate-Action from the RADIUS server.</p> <p>This attribute can be sent multiple times for different traffic classes. If Class is set to 0, it applies across all traffic classes.</p>



Type of Service/Traffic Class Configuration for Predefined Rules

- [Feature Summary and Revision History, page 759](#)
- [Feature Description, page 760](#)
- [How It Works, page 760](#)
- [Configuring the TOS/Traffic Class for Predefined Rules , page 762](#)
- [Monitoring and Troubleshooting, page 762](#)

Feature Summary and Revision History

Summary Data

Applicable Product(s) and Functional Area	<ul style="list-style-type: none">• GGSN• P-GW• SAEGW
Applicable Platform(s)	<ul style="list-style-type: none">• ASR 5500• VPC - DI• VPC - SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable

Related Documentation	<ul style="list-style-type: none"> • <i>Command Line Interface Reference</i> • <i>GGSN Administration Guide</i> • <i>P-GW Administration Guide</i> • <i>SAEGW Administration Guide</i>
-----------------------	--

Revision History

Revision Details	Release
First Introduced	21.3

Feature Description

A traffic flow template (TFT) is an information element that specifies parameters and operations for a Packet Data Protocol (PDP) context. This information element may be used to transfer extra parameters to the network (for example, the Authorization Token; see 3GPP TS 24.229 [95]). The TFT may contain packet filters for the downlink direction, uplink direction, or for both directions.

The packet filters determine the traffic mapping to PDP contexts. Ideally, the network uses the downlink packet filters while the mobile stations use the uplink packet filters. This behavior is also seen for a packet filter that applies to both the directions.

The TFT is a type 4 information element with a minimum length of 3 octets. The maximum length for the IE is 257 octets.

Currently, there is a requirement for an Operator to identify and filter data traffic based on the "Type of Service (TOS)/Traffic class" information. This information needs to be configured as part of the Predefined or Dynamic rules (or both). Also, the Operator wants to send "Type of Service (TOS)/Traffic Class" information as part of TFT in the Create Bearer Request (CBR) and Update Bearer Request (UBR) messages, which can be triggered via the Local Policy or PCRF.

For Dynamic rules, the P-GW already supports "Type of Service (TOS)/Traffic class" information that is used to identify specific data traffic. However, for Predefined rules, there is no option available to configure "Type of Service(TOS)/Traffic class" information as part of packet filter configuration.

This feature introduces the **ip tos-traffic-class** CLI to configure Type of Service (TOS)/Traffic class information in the packet filter configured under charging action to address the Operator requirements.

How It Works

The new CLI configures the packet filter associated with the Predefined rules, with the "Type of Service (TOS)/Traffic Class" configuration. These Predefined rules can be triggered via Local Policy or as part of PCRF communication.

The CLI syntax to configure "Type of Service (TOS)/Traffic Class" information under Predefined rules is in-line with "Type of Service (TOS)/Traffic Class" AVP information that is received as part of the Dynamic rules from PCRF.

According to 3GPPP 24.008 - Section 10.5.6.12, "For "Type of service/Traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet Type-of-Service/Traffic Class field and a one octet Type-of-Service/Traffic Class mask field. The Type-of-Service/Traffic Class field shall be transmitted first."

For example:

```
toS/traffic class: 0x20 0xff
```

Also, now the P-GW includes both the "Type of Service (TOS)/Traffic class" information under TFT IE, as part of the Create Bearer Request (CBR) and Update Bearer Request (UBR) messages (which is in line with 3GPP 29.212 Section 5.3.14).



Important

- The CLI is added in "packet-filter" configuration mode to configure TOS/Traffic class information.
- While triggering the Create or Update Bearer Request towards a peer, P-GW populates the "Type of Service (TOS)/Traffic class" information under TFT IE if the Predefined rule associated with that bearer is configured with "Type of Service (TOS)/Traffic class" information.
- There is no impact of Session Manager Recovery or ICSR on existing bearer packet filter information.

Limitations

Following are the limitations of this feature:

- Operator should configure TOS along with mask and there are no default values for TOS value and mask.
- For any change of "Type of Service (TOS)/Traffic class" configuration under packet filter, the behavior is in line with the other packet filter parameter configuration change.
- Current PGW/GGSN/SAEGW behavior is that if the Predefined rules installed on the different bearers have ToS/Traffic class configured for uplink traffic on one bearer and downlink traffic on another bearer, then uplink and downlink packets for the same flow go through different bearers accordingly. However, if these Predefined rules with configured ToS/Traffic class are removed on the fly, still uplink and downlink packets for the same flow will go through different bearers.
- Consider the scenario where there are two dedicated bearers installed with Predefined rules such that the uplink traffic with a particular ToS/Traffic class say t1, matches first dedicated bearer and the downlink traffic with another ToS/Traffic class say t2, matches downlink traffic. If the IP ToS/Traffic class CLI is disabled in the corresponding Predefined rules followed by SESSMGR restart, the downlink packets with ToS/Traffic class "t2" will go through the first dedicated bearer instead of second if there is an uplink packet with the same flow (source IP, source port, destination IP, destination port) received before this downlink packet.

Configuring the TOS/Traffic Class for Predefined Rules

The following section provides the configuration command to enable or disable the feature.

Enabling or Disabling the ip tos-traffic-class Command

The modified command, **ip tos-traffic-class**, is used to configure ToS/Traffic class under charging action in the Packet filter mode.

This CLI is disabled by default.

To enable or disable the feature, enter the following commands:

```
configure
  active-charging service service_name
    packet-filter packet_filter
      [ no ] ip tos-traffic-class { type_of_service | traffic class } mask { mask_value }
    end
```

Notes:

- **no** : If previously configured, deletes the ToS/Traffic class under charging action.
- **tos-traffic-class** = { *type_of_service* | *traffic class* } : Specifies the Type of Service (TOS)/Traffic Class" value that is used to filter the traffic. Enter an integer, ranging from 0 to 255.
- **mask** { *mask_value* } : Validates the dynamic rules for automatic recovery after a switchover. Enter an integer, ranging from 0 to 255.

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs in support of this feature.

Show Commands

This section lists all the show commands available to monitor this feature.

show configuration

This command has been modified to display the following output:

```
show configuration
configure
  active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      ip tos-traffic-class = 32 mask = 255
    exit
```

show active-charging packet-filter

This command has been modified to display the following output:

When ToS/Traffic class is enabled/configured:

```
show active-charging packet-filter { all | name }
Service Name: acs

Packet Filter Name: abcd
  IP Proto: 6
  Local Port: Not configured
  Remote Port: 226
  Remote IP Address: Not configured
  Direction: Bi-Directional
  Priority: None
  Tos-traffic-class: 32
  Tos-traffic-class-mask: 255
```

When ToS/Traffic class is disabled/not configured:

```
show active-charging packet-filter { all | name }

Service Name: acs

Packet Filter Name: abcd
  IP Proto: 6
  Local Port: Not configured
  Remote Port: 226
  Remote IP Address: Not configured
  Direction: Bi-Directional
  Priority: None
  Tos-traffic-class: Not configured
  Tos-traffic-class-mask: Not configured
```

show configuration verbose

This command has been modified to display the following output:

When ToS/Traffic class is enabled/configured:

```
show configuration verbose
configure
  active-charging service acs
  packet-filter PF226
    ip protocol = 6
    ip remote-port = 226
    ip tos-traffic-class = 32 mask = 255
  ---
  exit
```

When ToS/Traffic class is disabled/not configured:

```
show configuration verbose
configure
  active-charging service acs
  packet-filter PF226
    ip protocol = 6
    ip remote-port = 226
    no ip tos-traffic-class
  ---
  exit
```




Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

- [APN Engineering Rules, page 765](#)
- [DHCP Service Engineering Rules, page 765](#)
- [GGSN Engineering Rules, page 766](#)
- [GRE Tunnel Interface and VRF Engineering Rules, page 766](#)
- [GTP Engineering Rules, page 766](#)
- [Interface and Port Engineering Rules, page 766](#)
- [Lawful Intercept Engineering Rules, page 768](#)
- [MBMS Bearer Service Engineering Rules, page 768](#)
- [Service Engineering Rules, page 768](#)
- [Subscriber Engineering Rules, page 769](#)

APN Engineering Rules

The following engineering rules apply to APNs:

- APNs must be configured within the context used for authentication.
- A maximum of 2,048 APNs per system can be configured.

DHCP Service Engineering Rules

The following engineering rule applies to the DHCP Service:

- Up to 8 DHCP servers may be configured per DHCP service.
- A maximum of 3 DHCP server can be tried for a call.

GGSN Engineering Rules

The following engineering rules apply when the system is configured as a GGSN:

- Gn/Gp interfaces can be configured. That is, if a system context is configured with a GGSN service, then all interfaces in that context may be used.
- Gi interfaces can be configured. That is, if a system context is configured as a destination context for an APN, then all interfaces in that context may be used.
- Ga interfaces. That is, if a system context is configured for GTPP accounting, then all interfaces in that context may be used.
- One GSN-MAP node may be configured per system context (in lieu of Gc).
- Up to 1000 network requested PDP contexts may be configured.
- Up to 8 GTPP groups (excluding the default GTPP group) can be configured per chassis.
- Up to 4 GTPP Storage Servers can be configured per GTPP group.
- Up to 32 GTPP Storage Servers can be configured per system context.
- Up to 511 GRE tunnel interface can be configured per context.

GRE Tunnel Interface and VRF Engineering Rules

The following engineering rules apply to GRE tunnel interface and VRF contexts:

- A maximum of 511 GRE tunnels are allowed to configure in a context but subject to maximum of 2048 GRE tunnels per chassis.
- A maximum of 300 virtual routing and forwarding (VRF) tables are allowed to be configured in a context, subject to a maximum of 2,048 VRFs per chassis.
- A maximum of 10000 IP routes in Release 9.0 and 16384 IP routes in Release 10.0 onward are supported in a VRF context configuration mode.

GTP Engineering Rules

The following engineering rules apply to GTP on GGSN:

- A maximum of 11 primary (no secondary) PDP context per subscriber can be configured.
- A maximum of 1 primary and 10 secondary PDP context per subscriber can be configured.

Interface and Port Engineering Rules

The rules discussed in this section pertain to both the Ethernet 10/100 and Ethernet 1000 Line Cards and the four-port Quad Gig-E Line Card (QGLC) and the type of interfaces they facilitate.

Pi Interface Rules

This section describes the engineering rules for the Pi interface.

FA to HA Rules

When supporting Mobile IP, the system can be configured to perform the role of an FA, an HA, or both. This section describes the engineering rules for the Pi interface when using the system as a FA.

The following engineering rules apply to the Pi interface between the FA and HA:

- A Pi interface is created once the IP address of a logical interface is bound to an FA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within the egress context.
- FA services must be configured within the egress context.
- If the system is configured as a FA is communicating with a system configured as an HA, then it is recommended that the name of the context in which the FA service is configured is identical to the name of the context that the HA service is configured in on the other system.
- Each FA service may be configured with the Security Parameter Index (SPI) of the HA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the FA service to allow communications with multiple HAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited.

HA to FA

The following engineering rules apply to the Pi interface between the HA and FA:

- When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA or both. This section describes the engineering rules for the Pi interface when using the system as an HA.
- A Pi interface is created once the IP address of a logical interface is bound to an HA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within an ingress context.
- HA services must be configured within an ingress context.
- If the system configured as an HA is communicating with a system configured as a FA, then it is recommended that the name of the context in which the HA service is configured is identical to the name of the context that the FA service is configured in on the other system.
- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the Pi interface.

- Multiple SPIs can be configured within the HA service to allow communications with multiple FAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Each HA service must be configured with a Security Parameter Index (SPI) that it will share with mobile nodes.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited in order to allow higher bandwidth per subscriber.

GRE Tunnel Interface Rule

The following engineering rules apply to the GRE tunnel interface between two GRE tunnel nodes:

- A maximum of 512 IP tunnels (511 GRE tunnels + 1 not tunnel interfaces) are allowed to configure in a context but subject to a maximum of 2048 GRE tunnels per chassis.

Lawful Intercept Engineering Rules

The following engineering rules apply to Lawful Intercept on supported AGW service:

- A maximum of 1000 Lawful Intercepts can be performed simultaneously.

MBMS Bearer Service Engineering Rules

The following engineering rules apply to MBMS bearer services:

- A maximum 15 downlink SGSNs per MBMS bearer service are supported on ST16.
- A maximum 225 downlink SGSNs per MBMS bearer service are supported on the system.
- A maximum of 2 BMSC (1 primary and 1 secondary) supported per MBMS bearer service.

Service Engineering Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.



Caution

Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- Up to 2,048 MN-HA and 2048 FA-HA SPIs can be supported for a single HA service.

- Up to 2,048 FA-HA SPIs can be supported for a single FA service.
- The system supports unlimited peer FA addresses per HA.
- The system maintains statistics for a maximum of 8192 peer FAs per HA service.
- If more than 8192 FAs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer HAs per FA service.
- The total number of entries per table and per chassis is limited to 256.
- Up to 10,000 LAC addresses can be configured per LNS service.

**Caution**

Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty in troubleshooting the problems, and make it difficult to understand outputs of **show** commands.

Subscriber Engineering Rules

The following engineering rule applies to subscribers configured within the service:

- Default subscriber templates may be configured on a per FA service basis.

