S5800-24T8S Switch FSOS Software Release Notes

Models: S5800-24T8S

RELEASE NOTES

Contents

Chapter 1 Introduction

Current Release	FSOS- V7.5.1.R bin
Category	Firmware version

Chapter 2 New Changes

2.1 V7.5.1.R

New features	Specification
The Netconf architecture fault is rectified	N/A
Supports ED25519 format keys	N/A
Supports IPv6 cross-VNI route forwarding	N/A
CPU-TRAFFIC optimization (APP traffic)	N/A
The DHCP Server supports static IP binding for ports	N/A
The Route-map name is expanded from 20 characters to 63 characters	N/A
Run LLDP on the management interface	N/A
The 530 supports IPv6 BFD	N/A
680 LPM Specification Optimization &OSPFv3 performance Optimization	N/A
COPP supports whitelisting	N/A
(Stack)9slot(Demo)	N/A
ACCESS supports processing tag packets	N/A
The LLDP management address supports VRF	N/A

2.2 V7.4.12.R

New Features	Specification
SSH upgrade (OpenSSH upgraded to 9.8p1, OpenSSL upgraded to OpenSSL 1.1.1w).	N/A
MLAG supports MSTP.	N/A
PVLAN supports tagging	N/A
Stacking supports OSPF BFD.	N/A
SNMP trap supports specifying an IPv6 source address.	N/A
MIB supports interface CRC counters.	N/A
DHCPv4 relay/DHCPv6 relay supports specifying a source address.	N/A
HWMonitor supports average delay and timestamp reporting.	N/A
Supports 9-slot stacking (demo level).	N/A
BGP/OSPFv2 routing architecture optimization.	N/A
IGMP Snooping functionality optimization (industry requirement, implemented as a general feature).	N/A
(Stack) Supports controlling auto-merge and stack port optimization.	N/A

2.3 V7.4.11.R1.R

New Features	Specification
The L4 port is secure.	N/A
Supports periodic backup of configuration files to the tftp/ftp server.	N/A
Loopback internal optimization	N/A
The VxLAN network supports ECN.	N/A
Route-map can match extcommunity-list	N/A
The web supports time range/PoE.	N/A
IPSLA supports MTU detection.	N/A
Stacking supports NDP and IPv6 static routes.	N/A
Addded image encryption function.	N/A
Added the license file encryption function	N/A
The passive interface all configuration was added to OSPF.	N/A
The interface support ip/ipv6 address specifications increased (ipv4 support 64, ipv6 support 33)	N/A
Add license control for NETCONF and RPC.	N/A

2.4 V7.4.10.R1.R

New Features	Specification
In stacking, support IPV4 BFD linkage IPV 4 static routing	N/A
SSH supports lock source IP access control	N/A
ND Snooping supports 680	N/A
ACE supports Description	N/A
Support for PTP MIB	N/A

2.4 V7.4.10.R1.R

New Features	Specification
BGP IPv6 VRF supports aggregated routing	N/A
SNMP changes the source port number to support SNMPv3	N/A
PBR supports IPv6	N/A

2.5 V7.4.8.R

New features	Specification
Support BGP neighbor peer-group listen	Support to listen to the BGP connecting request of the specified network and establish the BGP neighbor automatically.
System security optimize	Support to display the SNMP community name with cipher text mode Support to display the password in log/history commands with cipher text mode Support to configure SSH protocol
Support to specify the VRF for NTP	N/A
Support to specify the VRF for logging server	N/A
Support user defined option fields for DHCPv4 server	Support class-map to match Traffic Class field in IPv6 packet without ACL.
Support to match the DSCP field of IPv6 packets	N/A
Support inband/outband SSH/SNMP protection for stacking	N/A
Route-map optimize	Support to set description string for route-map

Chapter 3 CLI Changes Specification

3.1 V7.4 .11 .R1.R

Original format	New Format	Remark
-	neighbor xxx as-origination-interval <0-600>	In the BGP view, configure the as-origination-interval <0-600> for neighbor xxx.
-	date-size <0-9172>	In the IPSLA view, configure data-size <0-9172>.
-	set-df	In the IPSLA view, configure set-df (only supported for IPv4).
-	ftp server acl	Add ftp server acl command.
-	passive-interface all/no passive-interface all	In the OSFP view, add this command.
loopback port loopback port mac-address swap	-	Delete these commmand lines.
-	remote-vtep <1-65535> encapsulation-ecn-strategy (ecn-copy|map|none)/no remote-vtep <1-65535> encapsulation-ecn-strategy	In the overlay review, add this command line.
-	encapsulation-ecn-strategy (ecn-copy|map|none)/no encapsulation-ecn-strategy	In the interface NVE view, add this commmand line.
-	-	The ES field is added in the show overlay remote-vtep display, and the abbreviation is changed by referring to the show overlay ipv6 remote-vtep display. The ES field is displayed show overlay ipv6 remote-vtep. The ES field is added to the show overlay evpn remote-vtep interface display, and the short format is changed by referring to the show overlay ipv6 remote-vtep interface display.
-	ip unreachables	Added ip unreachables to control whether ICMP unreachable packets are returned globally.

3.2 V7.4 .10 .R1.R

Original format	New Format	Remark
-	-	The command line neighbor XX:XX next hop carry-link-local is added to the BGP IPv6 address family to control whether the link-local address is carried in the update packet.
-	-	Add the command line ip mtu check enable/no ip mtu check enable to control whether the super interface MTU packets are sent to the CPU for processing, and the CPU is not used by default.

3.3 V7.4.8.R

Original format	New format	Remark
-	cpu threshold alarm ALARM restore RESTORE (slot SLOT |) no cpu threshold (slot SLOT |)	To configure cpu alarm value and restore value, use the this command in global configuration mode. To restore cpu alarm and restore threshold value to default, use the no form this command in global configuration mode.
-	show cpu threshold (slot SLOT)	To show configuration of cpu threshold, use the show cpu threshold command in privileged EXEC mode.
-	memory threshold alarm ALARM restore RESTORE (slot SLOT |) no memory threshold (slot SLOT |)	To configure memory alarm value and restore value, use the this command in global configuration mode. To restore memory alarm value and restore value to default, use the no form of this command in global configuration mode.
-	show memory threshold (slot SLOT)	To show configuration of memory threshold, use the show cpu threshold command in privileged EXEC mode.
-	description *LINE* no description *LINE*	Use this command in route-map mode to add description for route-map. Use the no form of this command to remove the description.
neighbor A.B.C.D fall-over bfd (multihop |) no neighbor A.B.C.D fall-over bfd (multihop |)	neighbor (A.B.C.D | X:X::X:X | WORD) fall-over bfd (multihop |) no neighbor (A.B.C.D | WORD) fall-over bfd (multihop |)	Support IPv6 BFD
neighbor IPADDRESS bfd interval { mintx TX_VAL | minrx RX_VAL | multiplier MULTI_VAL } no neighbor IPADDRESS bfd interval { mintxTX_VAL | minrx RX_VAL | multiplier MULTI_VAL }	neighbor (A.B.C.D | X:X::X:X | WORD) bfd interval { mintx TX_VAL | minrx RX_VAL | multiplier MULTI_VAL } no neighbor (A.B.C.D | X:X::X:X | WORD) bfd interval { mintx TX_VAL | minrx RX_VAL | multiplier MULTI_VAL }	Support IPv6 BFD
-	neighbor WORD peer-group listen (external | internal |) no neighbor TAG peer-group listen (external | internal |)	Use this command to create a peer-group for listen net. Use the no parameter with this command to disable this function

3.3 V7.4.8.R

Original format	New format	Remark
-	neighbor WORD listen-net (A.B.C.D/M | X:X::X:X/M) no neighbor WORD listen-net (A.B.C.D/M | X:X::X:X/M)	Use this command to create a listen net for the peer group. Use the no parameter with this command to disable this function
-	neighbor WORD listen-as [<1-4294967295>] no neighbor WORD listen-as [<1-4294967295>]	Use this command to create a listen as for the peer group. Use the no parameter with this command to disable this function
-	neighbor WORD listen-as-segment <1-4294967295> <1-4294967295> no neighbor WORD listen-as-segment <1-4294967295> <1-4294967295>	Use this command to create a listen as segment for the peer group. Use the no parameter with this command to disable this function
-	show ip bgp vpnv4 vrf NAME peer-group (WORD (summary |) |)	Use this command to display peer group specific information in vrf.
-	ipv6 ospf bfd (instance INSTANCE-ID |) no ipv6 ospf bfd (instance INSTANCE-ID |)	Use this command to enable BFD co-work with OSPFv3. Use the no form of this command to disable it.
ntp peer (HOSTNAME | IP_ADDR) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp peer (HOSTNAME | IP_ADDR)	ntp peer (mgmt-if | vrf NAME |) (HOSTNAME | IP_ADDR) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp peer (mgmt-if | vrf NAME |) (HOSTNAME | IP_ADDR)	Support to specify the VRF name for NTP
ntp server (HOSTNAME | IP_ADDR) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp server (HOSTNAME | SRC_ADDR)	ntp server (mgmt-if | vrf NAME |) (HOSTNAME | IP_ADDR) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp server (mgmt-if | vrf NAME |) (HOSTNAME | SRC_ADDR)	Support to specify the VRF name for NTP
ntp mgmt-if (enable | only) no ntp mgmt-if	-	Do not support this command to enable use management interface for NTP
match dscp DSCP_STR no match dscp DSCP_STR	match (ipv6 |) dscp DSCP_STR no match (ipv6 |) dscp DSCP_STR	Support to match IPv6 packets

Chapter 4 New Behaviors Specification

4.1 V7.4.11. R1.R

Item	Earlier Behavior	New Behavior
ERSPAN protocol type	ERSPAN protocol type	The ERSPAN protocol type is changed to 0x88be.
Queue Configuration	-	The queue is changed to the default 8 queue mode.
BGP Local Outgoing Routes with Zero Delay	-	BGP supports local outgoing routes to advertise updates with 0 delay (no delay).
Overlay Uplink	-	Overlay uplink enable on hidden interfaces; Use VXLAN uplink to control VXLAN and GENEVE. Use NVGRE uplink to control NVGRE.
Configuring ARP/ND	-	Configuring ARP/ND triggers (supporting PBR, OSPF, and ISIS).

4.2 V7.4.10.R1.R

Item	Earlier Behavior	New Behavior
Optimize BGP functionality	No functionality of republish of BGP; IPv6 BGP can control update packets; BGP cannot let Mars address check go	BGP republishes the local route, and the local BGP routing protocol surface shows that the next hop is 0.0.0.0 IPv6 BGP can control whether update packets carry link-local addresses or not BGP lets Mars address check go (192.0.0.0/8 network segment)
MTU messages	Super interface MTU packets are sent to CPU.	Super interface MTU packets are not sent to CPU by default and are forwarded directly.

4.3 V7.4.8.R

Item	New format	New Behavior
Expand the VLAN name length	The maximum length of VLAN name is 31 characters	The maximum length of VLAN name is 128 characters
Expand the VRF name length	The maximum length of VRF name is 16 characters	The maximum length of VRF name is 31 characters

Chapter 5 Fixed Problem

5.1 FSOS-V7.5.1.R

Problem Description	Occurred Condition
The isis database is abnormal.	-
The actual frequency of sending ptp sync packets is slightly different from the configured interval.	-
After a specified operation, traffic cannot be routed to the vxlan tunnel.	-
Description of interface configuration in Debian system, device crash.	-
After the system is started, you can log in to the device through SSH and save the configuration before and after the system is started. As a result, the device configurations are inconsistent before and after the system is started.	-
An error message is generated on the web interface when special characters are specified in time-range.	-
Symptom In a stack scenario, the group-speed behavior is abnormal.	-
If lacp is configured for ports with different rates, interfaces added later cannot be aggregated successfully.	-
In mlag scenarios, the lacp priority does not take effect.	-
The lsp pointed to the Layer-3 interface in down state.	-
The ISIS route cost was incorrectly calculated.	-
The log is not synchronized to the flash automatically after the timeout.	-
In stack scenarios, the display rate of the show interface stasus on port 25G is abnormal.	-
After the SSH login failed, the connection was disconnected and the stack split.	-
The dhcp relay cannot enter the vxlan tunnel.	-
Isisv6 reissues the ospfv3 route.	-

5.2 FSOS-V7.4.12.R

Problem Description	Occurred Condition
In specific configurations, the real address becomes unreachable (cannot be pinged) after configuring a virtual address.	-
BGP BFD failes to establish.	Multiple VLAN interfaces in different VRFs using the same IP address.
The web interface becomes unresponsive and fails to recover after deleting a VLAN interface.	-
Abnormal system splits.	When configuring dual-master detection in a stacking setup.
Specific NA packets cause a temporary failure of IPv6 neighbor functionality.	-
Local and remote Type 5 routes with the same prefix may cause a crash when Type 5 routes are updated.	In EVPN VXLAN scenarios.
Business traffic with EtherType 0x9009 is dropped abnormally.	-
MLAG flapping causes negotiation failures.	-
OSPF cost values are incorrect.	-
Traffic forwarded to a VPLS tunnel has unreasonable physical port reflective checks.	-
Switch power restart.	When Packets are sent to the CPU due to MTU reasons.
The device crashes sometimes.	When receiving large BFD packets.

5.3 FSOS-V7.4.11.r1.r

Problem Description	Occurred Condition
OSPF interworking with BFD fails to trigger ARP learning.	-
The json format specified by rpc-api is not returned.	-
The Radius authorization is invalid, but Telnet authorization succeeds.	-
In specific configurations, NETCONF cannot obtain device configurations.	-
The device occasionally prints an sdk error log.	-
The device experiences management disruption in some cases.	In a sustained SSH attack scenario, the device loses management connectivity.
The BGP peer is disconnected occasionally.	-
The device may crash.	Device crashes when using route-map to filter routes in VRF.
Unable to specify management port for Telnet login to other devices on Debian.	When using Telnet from a Debian system to log into other devices.
BFD binding to VRF fails to establish session with devices of the same series, when stacking wth other models, including S5850-48B8C, S5850-48B8C-PE, S8550-32C, S8550-32C-PE, S8550-16Q8C, S5850-48S6Q-R, S5850-48S6Q-R-PE.	-
In specific scenarios, the DHCP server is unable to allocate an IP address.	-
Switch cannot handle 256-color terminal types.	Error when logging into the switch via SSH using a terminal of type xterm-256color.
The source option may become invalid.	After specifying the TACACS server key, the source option becomes invalid.
Repeatedly reapplying the configuration causes the stack backup board to lose connectivity.	Repeatedly reapplying or resetting the configuration on a stacked network device.
The MLAG neighbor relationship is restored in some cases.	The MLAG neighbor relationship is reestablised, because the BGP neighbor relationship is disconnected.
Editing all ports through the web interface causes the web interface to freeze and become unresponsive, unable to recover.	When making bulk changes to all network ports through the web management interface.
The interface's real address cannot be pinged.	After configuring a virtual address, the interface's real address cannot be pinged.
Stack configuration may lead to a split.	After the stack configuration is performed, the keepalive timeout of the stack system causes the stack split.
Deleting the VLAN from the Web UI prevents card recovery.	After the VLAN if is deleted from the Web UI, the card cannot be recovered.
In certain scenarios, BGP BFD is enabled, and the BFD session is not UP.	-

5.4 FSOS-V7.4 .10.R1.R

Problem Description	Occurred Condition
In certain cases,devices receive the abnormal IGMP Report message and the devices crash in S5850 series.	-
Configuration interfaces leave residue in S5850 series.	Residue after interface configuration under specific operation.
Devices crash under FDB drift scenario in S5850 series.	Crash of devices under FDB drift scenario.
In certain cases, memory leaks in S5850 series.	Executing specific commands via RPC.
The address pool range configured by the device as a DHCP server is not fully valid in S5850 series.	-
Common node return values of LLDP does not conform to the standard behavior in S5850 series.	-
RP port receives repeated Proposal message, DP enters the state of discarding, RP has completed PA negotiation, and DP initiates PA negotiation to downstream devices again, causing network oscillation in S5850 series.	-
Devices disconnect from BGP in S5850 series.	Receiving specific BGP message

5.5 V7.4.8.R

Problem Description	Occurred Condition
Port-bridge does not work in some case	When there are large number of VLAN configured on the system, port-bridge only take action on part of the VLANs.
Specific operation may lead system crash	Use the "show interface" command continuously can lead memory leak. The memory may exhaust and lead system crash finally
Specific operation may lead BGP work abnormal	System may parse BGP open packets error which lead process busy and system crash with a small probability
The management interface failed to get the default route by DHCP during smar-config period	Enable DHCP on the management interface, then reboot the system and use smart-config
The port mirror does not work after system reboot in some case	The mirror source is dynamic aggregator, the mirror does not work after system reboot.
Specific operation may lead WEB access abnormal	Several users access the WEB and operate on the WEB at same time may lead WEB abnormal.