S5800 Series Switches

FSOS Software Release Notes

Models: S5800-48F4SR; S5800-48T4S; S5800-48F4SR-DC; S5800- 48T4S-DC; S5800-48T4S-PE

RELEASE NOTES

Contents

Chapter 1 Introduction

1.1 Basic Information

Current Release	FSOS-V7.5.6
Category	Official release

Chapter 2 New Changes

2.1 V7.5.6

New features	Specification
LLDP feature optimization	LLDP neighbor optimization LLDP MED TLV optimization
Support GVRP	N/A
DHCP Option 82 feature optimization	N/A
IP Source Guard feature optimization	Support global IP Source Guard
Port Security feature optimization	Support sticky mac
Storm control feature optimization	Support errdisable
VXLAN micro-segmentation support	N/A

2.2 V7.5.5

New features	Specification
MLAG supports multicast	MLAG supports the synchronization of IGMP snooping entries.
Optimize VPLS performance	Optimize failure switchover performance
DHCP address pool supports binding to VRF	Support binding DHCP address pools to non-default VRF
Support ARP proxy in stacking environments	Support local-proxy-arp and proxy-arp

2.3 V7.5.4.r2

New features	Specification
Added a multicast parameter configuration	Introduced the Max Response parameter to improve configuration

section to the Web interface	convenience for users

2.4 V7.5.4.r1

New features	Specification
Optimize the convergence behavior of remote LDP sessions	Improve VPLS/VPWS convergence performance during link failures

2.5 V7.5.4

New features	Specification
Voice VLAN Optimization	Voice VLAN replaces DSCP. DSCP can only be modified if DSCP replacement is enabled on the egress. When the egress is a route-port, DSCP cannot be modified.
Supports the use of DHCPv6 functionality under the MPLS profile.	N/A
Support displaying the default configuration.	Use the show this all and show running-configure all commands to display the default configuration.
WEB UI optimization	Support displaying a progress bar when uploading files
The stacking system supports DHCPv4 server	N/A
MIB now supports the Mirror Mult-Dest node	OID: 1.3.6.1.4.1.27975.3.6
Support multi-device stacking.	Supports up to 4 devices

2.6 V7.5.3.r2

New features	Specification
Support security reminder	Support reminder user to change the default username and password
Support ECN statistics	Support statistics in VxLAN network
WEB jQuery optimized	Update jQuery version for fix the known flaw
Support gNMI Telemetry	N/A
Support flow control statistics on MIB	N/A
Support configure LACP on WEB UI	N/A

Support I2C isolation	When a problematic optical module lead the interface abnormal, other interfaces are not affected
Support Jumbo frame command	Support jumbo frame command. But do not support for stacking
Support DHCPv6 Server	N/A
Support authentication for gRPC	N/A
Support PFC watermark	N/A
Support routes cross VRFs	Support routes cross VRFs by BGP
Support IPv6 ECMP PBR	N/A
Support new MIB OID: ifConnectorPresent	Use this OID to get if the interface is physical or logical
Support new features on stacking	Support following new features in stacking environment: IPv6inv4 Tunnel ND Snooping OSPFv3 PFC VLAN policer Prefix-list Routemap IPv6 PBR Web UI
Layer 2/3 multicast optimized	When layer 2 and layer 3 IGMP enabled together, the group entries aging time keep coincident
Support new MIB OIDs for OSPF	Support to create and delete OSPF instance and configure networks by SNMP
Support entries ageing in batching for ARP and ND	By default, 200 ARP entries and 100 ND entries are ageing in one minute

2.7 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	N/A

ports	
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

2.8 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

2.9 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

2.10 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
BGP IPv6 VRF supports aggregated routing	N/A
SNMP changes the source port number to support SNMPv3.	N/A
PBR supports IPv6.	N/A

2.11 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	Support class-map to match Traffic Class field in IPv6 packet without

server.	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 V7.5.6

Original format	New Format	Remark
-	show processes cpu core history (slot ID |)	To display CPU core utilization information for a period of time, use the show processes cpu core history command in Privileged EXEC mode, the period of 1s, 1min, 5min could be shown.
errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection) no errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection)	errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection | storm-control) no errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection | storm-control)	Storm control supports placing the interface in errdisable state when the threshold is exceeded.
-	storm-control action (suppress | errdisable) no storm-control action	Use this command to configure storm control actions on layer 2 port. Use the no form of this command to return to the default setting.
-	New chapter: <GVRP>	Support GVRP
-	dhcp relay information option (circuit-id | remote-id) format extend no dhcp relay information option (circuit-id | remote-id) format extend	In global configuration mode, use the dhcp relay information option format extend command to enable the extended format for DHCP relay Circuit-ID or Remote-ID, so that the added Circuit-ID or Remote-ID content in packets includes Type and Length attributes. Use the no form of this command to disable this function.
-	clear port-security address-table sticky (interface IFNAME | vlan VLAN_ID | address	Use this command to clear sticky port-security mac address table.

	MAC_ADDR |)	
-	switchport port-security mac-address sticky no switchport port-security mac-address sticky	To enable port security sticky mac on an interface, use the switchport port-security mac-address sticky command. To disable port security sticky mac , use the no switchport port-security mac-address sticky.
show port-security address-table (static | dynamic |) (interface IFNAME | vlan VLAN_ID | address MAC_ADDR |)	show port-security address-table (static | dynamic | sticky |) (interface IFNAME | address MACADDR |) (vlan VLAN_ID |) (count |)	-
-	dhcp snooping information option (circuit-id | remote-id) format extend no dhcp snooping information option (circuit-id | remote-id) format extend	To enable the system to insert “type” and “length” attibutes in the content of suboption circuit-id or remote-id, use the dhcp snooping information option format extend command in global configuration mode. To disable inserting “type” and “length” attibutes in the content of circuit-id or remote-id , use the no form of this command.
-	ip source guard mode (port-only | global)	Use the "ip source guard mode" command to switch between global and interface-based IPSG modes.
-	radius-server attribute message-authenticator access-request no radius-server attribute message-authenticator access-request	To configure the device to include the Message-Authenticator attribute when sending RADIUS authentication packets, use the radius-server attribute message-authenticator access-request command in global configuration mode. To restore the default, use the no form of this command.
-	New chapter: <Micro segment>	Support Micro segment

3.2 V7.5.5

Original format	New Format	Remark
no line-secret	no secret	The SHA256 encrypted password hidden

		by using the "no secret" command.
show mac address-table (dynamic | static | multicast |) (address *MAC_ADDR* | interface *IFNAME* | vlan *VLAN_ID* |)	show mac address-table (dynamic | static | multicast |) (address *MAC_ADDR* (vlan *VLAN_ID* |) | interface *IFNAME* (vlan *VLAN_ID* |) | vlan *VLAN_ID* |) (count |)	When displaying MAC address table entries, support more filter condition combinations. Support using the count parameter to display the number of entries.
clear arp-cache ((vrf *VRF-NAME* |) interface *IFNAME* |)	clear arp-cache ((vrf *VRF-NAME* |) interface *IFNAME* | all |)	Support using the all parameter to update all ARP caches.
show ip arp (vrf *VRF-NAME* |) summary	show ip arp (vrf *VRF-NAME* | all |) summary	Support using the all parameter to view statistics of all ARP table entries.
-	vrf *WORD* no vrf	In address pool configuration mode, use the command vrf to configure the VPN instance under the address pool. Use the no form of this command to delete the configuration.
dhcp excluded-address *A.B.C.D* [*A.B.C.D*] no dhcp excluded-address *A.B.C.D* [*A.B.C.D*]	dhcp excluded-address (vrf *WORD* |) *A.B.C.D* [*A.B.C.D*] no dhcp excluded-address (vrf *WORD* |) *A.B.C.D* [*A.B.C.D*]	DHCP supports specifying a non-default VRF.
show dhcp server conflict [ip *A.B.C.D* | all]	show dhcp server (vrf *WORD* |) conflict [ip *A.B.C.D* | all]	DHCP supports specifying a non-default VRF.
show dhcp server binding [ip *A.B.C.D* | pool *WORD* | all]	show dhcp server binding [ip *A.B.C.D* | pool *WORD* | all] show dhcp server (vrf *WORD*) binding (ip *A.B.C.D* | all)	DHCP supports specifying a non-default VRF.
clear dhcp server conflict [ip *A.B.C.D* | all]	clear dhcp server (vrf *WORD* |) conflict [ip *A.B.C.D* | all]	DHCP supports specifying a non-default VRF.
clear dhcp server binding [ip *A.B.C.D* | pool *WORD* | all]	clear dhcp server binding [ip *A.B.C.D* | pool *WORD* | all] clear dhcp server (vrf *WORD*) binding (ip *A.B.C.D* | all)	DHCP supports specifying a non-default VRF.

3.3 V7.5.4

Original format	New Format	Remark
show this	show this (all |)	View configuration information including

		default settings
show running-config	show running-config (all |)	Use this command to set the DSCP for packets via Voice VLAN
-	voice vlan set dscp to DSCP no voice vlan set dscp	Use this command to enable Voice VLAN DSCP replacement on a port
-	voice vlan replace-dscp no voice vlan replace-dscp	Use this command to configure an IPv6 group
-	ipv6-group NAME (vrf WORD |) (load-share |) no ipv6-group NAME	Use the corresponding no command to delete the IPv6 group
-		
-	member ipv6 X:X::X:X (interface IFNAME |) (priority <0-65535> |) no member ipv6 X:X::X:X (track |)	Use this command to configure IPv6 group members. Use the corresponding no command to delete this rule
-	show ipv6-group (NAME |)	Use this command to display detailed information about the IPv6 group configuration
-	macsec include-sci no macsec include-sci	Used to configure whether MKA packets carry the SCI
-	mka timer mka-life TIME no mka timer mka-life	Used to modify the mka-life timer
-	mka timer sak-life TIME no mka timer sak-life	Used to modify the sak-life timer
termperature LOW HIGH CRITICAL no termperature	termperature LOW HIGH CRITICAL (slot ID |) no termperature (slot ID |)	The ID refers to the member ID in a stacking scenario; slot ID is not supported in non-stacking scenarios
fan BOTTOM_SPEED_RATE LOW_SPEED_RATE HIGH_SPEED_RATE FULL_SPEED_RATE no fan speed-rate	fan BOTTOM_SPEED_RATE LOW_SPEED_RATE HIGH_SPEED_RATE FULL_SPEED_RATE (slot ID |) no fan (slot ID |)	The ID refers to the member ID in a stacking scenario; slot ID is not supported in non-stacking scenarios

3.4 V7.5.3.r2

Original format	New Format	Remark

-	clear startup-config	To delete flash:/startup-config.conf file
-	format boot	format flash:/boot
-	start vct interface IFPHYSICAL	start get vct information for electrical(RJ45) ports
-	show virtual-cable-test interface IFPHYSICAL	start get vct information for electrical(RJ45) ports
-	ipv6 nd stale-time STALE_TIME no ipv6 nd stale-time	Use this command to set stale time of the neighbor entries. To restore the default configuration, use the no form of this command.
-	Add new chapter for “DHCPv6 Server Commands”	Support DHCPv6 Server
-	import-rib public (route-map RMAP |) no import-rib public (route-map |)	Use this command to import routes from BGP public routing-table to specified BGP vrf routing-table. Use the no parameter with this command to cancel the importing.
-	import-rib vrf NAME (route-map RMAP |) no import-rib vrf NAME (route-map |)	Use this command to import routes from specified BGP vrf routing-table to BGP public routing-table. Use the no parameter with this command to cancel the importing.
-		
-	ipv6 ospf restart enable no ipv6 ospf restart enable	To enable ospfv3 graceful restart function, use the command in global configuration mode. To disable the ospf GR, use the no form of this command.
-	ipv6 ospf restart helper enable no ipv6 ospf restart helper enable	To enable ospfv3 graceful restart helper function, use the command in global configuration mode. To disable this, use the no form of this command.
-	ipv6 ospf restart grace-period SECONDS no ipv6 ospf restart grace-period	To set ospfv3 graceful restart period, use the command in global configuration mode. To recover default value, use the no form of this command.
-	priority-flow-control buffer priority <0-7> xoff <MIN-MAX> xon <MIN-MAX> no priority-flow-control buffer priority	Use this command to configure PFC Xoff/Xon threshold for a physical port in absolute value mode. To unset port pfc threshold, use

	<0-7>	the no form of this command.
-	flowcontrol buffer xoff <MIN-MAX> xon <MIN-MAX> no flowcontrol buffer	Use this command to configure FC Xoff/Xon threshold for a physical port in absolute value mode. To unset port fc threshold, use the no form of this command.
mka policy NAME no mka policy NAME	mac-security-profile name NAME no mac-security-profile name NAME	
replay-protection enable no replay-protection enable	macsec replay-protection enable no macsec replay-protection enable	
replay-protection window-size SIZE no replay-protection window-size	macsec replay-protection window-size SIZE no macsec replay-protection window-size	
validation-mode (check | strict) no validation-mode	macsec validation-mode (check | strict) no macsec validation-mode	
icv-mode (normal | integrity-only) no icv-mode	macsec mode (none | normal | integrity-only) no macsec mode	
confidentiality-offset (0 | 30 | 50) no confidentiality-offset	macsec confidentiality-offset (0 | 30 | 50) no macsec confidentiality-offset	
mka apply policy NAME no mka apply policy	mac-security-profile NAME no mac-security-profile	
macsec icv-mode (normal | integrity-only) no macsec icv-mode	macsec mode (none | normal | integrity-only) no macsec mode	
macsec desire no macsec desire	Deleted	
mka priority PRIORITY no mka priority	mka keyserver priority PRIORITY no mka keyserver priority	
mka psk cipher-suite (gcm-aes-128 | gcm-aes-256) ckn CKN cak simple CAK mka psk cipher-suite (gcm-aes-xpn-128 | gcm-aes-xpn-256) ckn CKN	macsec cipher-suite (gcm-aes-128 | gcm-aes-256) macsec cipher-suite (gcm-aes-xpn-128 | gcm-aes-xpn-256) no macsec cipher-suite	Macsec optimized and command update

cak simple CAK		
-	show mka interface (IFNAME |)	To show MKA information.
-	fan BOTTOM_SPEED_RATE LOW_SPEED_RATE HIGH_SPEED_RATE FULL_SPEED_RATE no fan speed-rate	To set fan speed.
-	show resource overlay	Use this command to display the overlay resource information.
-	vlan VLAN_ID aliasing-disable	Use the command to disable aliasing. Use the no form of this command to remove the configuration.
-	esi VAL no esi	Use this command to set ethernet segment identifier.
-	evpn df-election preference PREFERENCE no evpn df-election preference	Use this command to set ethernet segment identifier.

3.5 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>	In the overlay review, add this command line.

	encapsulation-ecn-strategy (ecn-copy|map|none)/no remote-vtep <1-65535> encapsulation-ecn-strategy	
-	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.

3.6 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.

3.7 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 { mintx TX_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
-	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>	Use this command to create a listen as segment for the peer group.

	no neighbor WORD listen-as-segment <1-4294967295> <1-4294967295>	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 V7.5.6

Item	Earlier Behavior	New Behavior
switchport port-security maximum	Enforces the maximum limit affected dynamic entries	Now enforces the maximum limit on static port-security MAC address entries
VLAN Security/Port Security: Behavior Change for Modifying the MAC Address Limit	If the modified limit is smaller than the number of currently learned MAC addresses, automatically delete the learned MAC address entries and relearn	If the modified limit is smaller than the number of currently learned MAC addresses, return an error and disallow the modification

4.2 V7.5.5

Item	Earlier Behavior	New Behavior
Expand MAC address capacity	Maximum support for 96K MAC address table entries	Maximum support for 120K MAC address table entries.
Expand ND capacity	IPv6 profile supports 4K ND entries	IPv6 profile supports 6K ND entries.
Modify port security and VLAN security behaviors	Modify the behavior of the maximum number of dynamically learned addresses as follows: If the modified number is greater than the number currently learned, MAC address table entries will not be deleted and relearned	The behavior for modifying the maximum number of dynamically learned addresses is as follows: if the modified number is smaller than the currently learned quantity, delete the MAC address table entries and relearn them.
Optimize IP ARP display results	Do not distinguish between dynamic and static ARP	Dynamic and static entries are distinguished during display and can be filtered by parameters.
Modify the default number of stacking members	Default number of members is 2	The default number of members is 4.

4.3 V7.5.4

Item	Earlier Behavior	New Behavior
Static ARP-triggered EVPN	Static ARP-triggered EVPN routing not	Static ARP-triggered EVPN routing

routing	supported	supported
IPv6 source guard specification change	Previous specification: 128	Updated specification: 124
BGP default route behavior change	Advertises routes with 0.0.0.0 with any mask	Advertises only the 0.0.0.0/0 route

4.4 V7.5.3.r2

Item	Earlier Behavior	New Behavior
DHCP-Relay support normal and VXLAN route at same time	Do not support forwarding at same time	DHCP-Relay support normal and VXLAN route at same time
Giants frame statistic rule optimized	Packet size large than 1518 or CRC error frames statistic as Giants frames	Only the packets length large than jumbo frame should statistic as Giants frames
Queue limit display optimized	The queue limit display as “maximum” when the value is large than 8192	The queue limit value displays the real value
VXLAN EVPN behavior changes	Remote type2 use ARP entries	Remote type2 use route entries
RPC function behavior changes	Enable RPC service will occupy a VTY resource, which will lead the user login to the command/web UI reduced by 1	Enable RPC service will not occupy any VTY resource

4.5 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 IS-IS).

4.6 V7.4.10. R1.R

Item	Earlier Behavior	New Behavior
The display result changes for BGP redistributing local route	Display the actual nexthop address.	Display the nexthop address as “0.0.0.0”
The behavior changes for BGP network 192.0.0.0/8	BGP can not learn the route in this network	BGP can learn the route in this network.
The behavior changes for the service packets exceed the interface MTU size	System send the packet exceed the MTU to CPU and the CPU deal with the packets’ fragment.	System forward the packet exceed the MTU by default. User can enable or disable CPU fragment by command.

4.7 V7.4.8.R

Item	Earlier Behavior	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 V7.5.6

Problem Description	Occurred Condition
Under specific circumstances, the MLAG peer tunnel-side MAC is cleared after the tunnel is established	On MLAG devices with no sync-overlay configured, a local clear ip bgp operation may incorrectly delete EI MAC address entries on the peer device.
Under specific circumstances, the tunnel status becomes abnormal and the BGP process may crash	Enabling the device's “debug bgp” switch may cause a system crash.
Under specific circumstances, errors occur when creating or deleting aggregate ports	A persistent fdb-loop in the MLAG environment causes abnormalities in aggregate port creation/deletion.
Under specific circumstances, packets are encapsulated with an incorrect VNI	When acting as a centralized VXLAN Layer 3 gateway, after a host ARP is learned, modifying the VLAN-to-VNI mapping to a new VNI may cause traffic to be incorrectly encapsulated and forwarded with the old VNI.
Under specific circumstances, the device repeatedly enters the smart config process, resulting in a longer startup time	N/A
Under specific circumstances, UDF ACL does not take effect	When a user-defined access-list is applied first and then updated, the updated content does not take effect.
Under specific circumstances, inter-VRF ARP leaking causes a system crash	If the leaked ARP has the same prefix as a static route, there is a certain probability of causing system abnormalities or even a crash.
Under specific circumstances, waterline configuration fails	Interface PFC Waterline cannot be configured when DCBX negotiation is unsuccessful.

5.2 V7.5.5

Problem Description	Occurred Condition
Under specific circumstances, VPLS tunnel establishment fails.	The VPLS instance is configured with a non-default MTU. After first configuring a non-existent neighbor and then configuring an existing neighbor, the existing neighbor fails to come up.
Under specific circumstances, a port cannot join the same stacking port.	When port rates are inconsistent, they cannot be added to the same stacking port.
Under specific circumstances, an error occurs when the RPC-API enters the aggregated interface view.	After entering the physical interface configuration view via RPC-API, entering the aggregated interface view results in an error.
In specific network topologies, FTN entries are incorrectly delivered.	On the remote target peer device, an IP address in the same subnet as the interface of the local neighbor device was incorrectly configured. After this address was deleted, the related FTN entries were not restored.
When the next-hop route in the L3VPN public network has a non-32-bit mask, CE-side management becomes unreachable.	N/A
In VXLAN scenarios, specific operations cause the BGP process to crash.	When configuring VXLAN EVPN, overlay is enabled for multiple VLANs, and virtual IP addresses are configured on these interface VLANs along with a globally configured virtual address. Repeatedly adding and deleting the virtual addresses on an interface VLAN on one of the devices may cause the BGP process to crash with a certain probability.

5.3 V7.5.4.r2

Problem Description	Occurred Condition
The power value displayed in the show poe summary	N/A

command output is incorrect.	
The configurable parameter range of the multicast command igmp snooping querier tcn query-interval is unreasonable.	N/A

5.4 V7.5.4

Problem Description	Occurred Condition
Under certain conditions, in an L3VPN scenario, the PE cannot reach the remote private network address via the default route of the private network.	In an L3VPN scenario, when the PE uses the specified local VRF loopback address as the source IP and the remote private network address as the destination IP, packets cannot be sent out when matching the default route.
Under certain conditions, route flapping causes MPLS ILM table anomalies and packet loss.	During route convergence or reconvergence, there is a certain probability of MPLS ILM anomalies.
In a VXLAN scenario, MAC table entries may age abnormally and be cleared, leaving residual entries in the underlying layer.	In a VXLAN scenario, when learned MAC addresses are cleared, there is a certain probability of causing MAC table anomalies.
Under certain conditions, when private network packets contain directly connected network segments, local ARP learning is not triggered, resulting in traffic interruption.	Traffic originating from a VPN cannot trigger the locally directly connected device to initiate ARP requests.
MACsec interoperability with third-party devices fails under specific scenarios.	MKA packets sent by third-party devices include the ICV indicator field and are mistakenly identified as invalid packets, preventing successful establishment of the MKA session.

5.5 V7.5.3.r2

Problem Description	Occurred Condition
802.1x relay works abnormal in some case.	When the client send a packet with specified fields, 802.1x relay may filter these fields and lead authentication failed.

In L3VPN environment, traffic in remote private network cannot trigger ARP request in local private network, it may lead to network disconnection.	N/A
Radius server source-interface option takes no effect with specific configuration.	Configure key and source-interface together for one radius server, source-interface option takes no effect.
Interface can not up in some case	Clear the configuration of the interface and insert a 100G DAC module, the interface is up. Then replace the 100G module with a 200G DAC module. The plug out the 200G module and insert the 100G module again, the interface is always down.
In some case the tunnel head copy abnormal	When MLAG EVPN use same RD, withdraw the route may lead tunnel head copy status change to “disable”
Can not configure ACL by RPC-API	N/A
The terminal devices use traceroute to detect VxLAN layer3 gateway, the first hop information can not display	N/A
Route leak cross VRF works abnormal	If the leaked route is a default route, the traffic can not forward according this leaked route
Mirror feature abnormal in some case	The mirror source is VLAN interface in VRF. The interface destination is a group. Remove the mirror and VLAN interface and VLAN, then configure again, the mirror can not work
There are abnormal log in some case	UDP port 514 is attacked may lead abnormal log on system
The show interface result is not complete in some case	When the system memory is very high, the show interface result is not complete
Memory usage rises continuously in some case	Send specified LLDP packet to the device may lead memory leak
After master-slave witch over，the packets exceed the MTU size are not fragmented.	N/A
MLAG disconnected in some case	The command “acl-statistics exclude-drop enable” may lead MLAG disconnected
BGP update packet abnormal in some case	When the BGP route count is up to a certain number, the fields in BGP update packet are wrong
The devices may be out of management and out of service with a small possibility in some case	Continuous SSH attacks to the device may lead this issue
Vtep underlay route abnormal, pointer to a wrong	OSPF status flapping and the underlay route switches

nexthop	between default route and OSPF route for several times may lead nexthop abnormal with a small probability
In the MLAG environment, the device may occasional abnormal reboot.	In the MLAG environment. there are a large number of ARP attack the device, may lead the device reboot with a small probability
When modifying the description of the stack port in the WEB UI, an error occurred.	N/A
The terminal and the gateway obtained through slacc cannot communicate with each other.	After configuring the IPv6 virtual address, the gateway address obtained by the terminal through slacc are not reachable
The PTP sync statistics are wrong in some case	After enabling the fast packet configuration mode, the sync count will no longer increase.
The LDP label distribution is abnormal in some case	When the same FEC exists, the new and old LDPs alternate in distributing and releasing labels, which has a certain probability of causing label residue and distribution abnormal.
When EVPN receives a specific message, there is a certain probability that it will encounter an abnormality, resulting in incorrect routing distribution.	If unsupported types are included in the message, an error will occur during parsing.
On the WEB UI, the port status display on the STP page is incorrect.	N/A
The status of the VLAN interface changes unexpected in some case	When adding a VLAN to the trunk port through the WEB UI, due to the method of deleting and adding, the status of the VLAN interface experienced a change from being down to up.
The SNMP process crashes and the device restarts in some case	In stacking environment, if a read-only community is configured and then an SNMP-set operation is performed, there is a certain probability that it will cause the SNMP process crash
The storm control speed limit value was abnormally modified in some case	Configure the port for storm control, and then shut down the port. Using the "show interface xxx" command to view the status of this interface will cause the speed limit value for storm control to be set to 0.
The LDP session keeps flapping for a long time, and there is a certain probability that it will cause the cache area to be full and the system to crash.	N/A

5.6 V7.5.1.R

Problem Description	Occurred Condition
ISIS route abnormal in some case.	Use the “passive-interface” command without specify the interface name in “router isis” mode, enable all interfaces as isis passive-interface, include the Loopback interface. Change the ISIS metric-style as wide and then restore the metric-style to default， the LSP type will be wrong type.
Specified configuration may lead VXLAN tunnel traffic abnormal.	Add and remove the route and tunnel repeatedly, and send ARP packet continuously to learn the tunnel side ARP during processing the route and tunnel, may lead the system abnormal and discard the tunnel traffic. When tunnel ARP is existed, add and remove the route repeatedly and delete the FDB also has some property to lead the same abnormal phenomenon above.
Configuring interface description may lead system crash in Debian system	N/A
Specified process may lead configuration lost	The device has large amount of configurations and need a long time to load the configurations after system reboot. When the system is still loading the configurations, User can access the device via SSH and use “write” command to save the configuration, then the configurations not loaded are lost.
WEB UI report an error in some case	Use characters with specified usage in http language for the name of time-range will lead the WEB UI report error
Group speed abnormal in stacking environment	The slave and master are both S5850-16T16BS2Q.
Configure the interface with different speed as LACP，the member failed to join the aggregator	N/A
LACP priority and MLAG priority are not coincide in some case.	Disable MLAG and change the LACP priority， then enable MLAG，the LACP priority and MLAG priority are not coincide

The status of layer 3 aggregator is down， the previous LSP may still point to this aggregator and lead traffic discard.	N/A
ISIS route cost is wrong when redistribute the routes.	N/A
The log may not write to the flash in some case	User login/logout the device frequently or change the log related configurations may lead some log failed to write the flash, with a small probability.
“Show interface status” rate abnormal for 25G interfaces in stacking environment	N/A
After SSH login failed and disconnected, the stack may split into two devices with a small probability.	After input wrong username and password to SSH terminal and login the device failed, the stack may split into two devices with a small probability. Part of SSH terminal have this problem.
DHCP relay in VXLAN environment works abnormal.	Underlay output interface is connected ARP, DHCP discover packet can not forwarding according the DVR route
ISISv6 redistribute OSPFv3 route abnormal	N/A
The actual frequency of sending ptp sync packets is slightly different from the configured interval.	N/A

5.7 V7.4 .12.R

Problem Description	Occurred Condition
In specific configurations, the real address becomes unreachable (cannot be pinged) after configuring a virtual address.	N/A
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.	N/A

Abnormal system splits.	When configuring dual-master detection in a stacking setup.
Specific NA packets cause a temporary failure of IPv6 neighbor functionality.	N/A
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.	N/A
MLAG flapping causes negotiation failures.	N/A
OSPF cost values are incorrect.	N/A
Traffic forwarded to a VPLS tunnel has unreasonable physical port reflective checks.	N/A
Switch power restart.	When Packets are sent to the CPU due to MTU reasons.
The device crashes sometimes.	When receiving large BFD packets.
BGP neighbor state flaps when receiving IPv6 EVPN routes.	The received IPv6 EVPN routes cannot be processed, causing the neighbor to time out, disconnect, and reconnect repeatedly.

5.8 V7.4 .11.r1.r

Problem Description	Occurred Condition
OSPF interworking with BFD fails to trigger ARP learning.	N/A
The json format specified by rpc-api is not returned.	N/A
The Radius authorization is invalid, but Telnet authorization succeeds.	N/A
In specific configurations, NETCONF cannot obtain device configurations.	N/A
The device occasionally prints an sdk error log.	N/A

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.	N/A
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.
FD 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.	N/A
In specific scenarios, the DHCP server is unable to allocate an IP address.	N/A
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.	N/A

5.9 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.	N/A
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.	N/A
Common node return values of LLDP does not conform to the standard behavior in S5850 series.	N/A
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.	N/A
Devices disconnect from BGP in S5850 series.	Receiving specific BGP message

5.10 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.