S5850-48B8C and S5850-48B8C-PE Switches FSOS Software Release Notes (V7.4.8.r and Above)

Models: S5850-48B8C; S5850-48B8C-PE

RELEASE NOTES

Contents

Chapter 1 Introduction

Current Release	FSOS-V7.5.5.bin
Category	Firmware version
MD5	4c3db8e616d82d4590b915a202f846e9

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
Support batch hot splitting	The split command supports specifying a port range

2.3 V7.5.4.R2

New Features	Specification

Support multicast parameter configuration on WEBUI	Support new parameter “max response” on WEBUI to enhance user configuration convenience
Remote LDP session convergence optimized	Optimize the VPLS/VPWS convergence performance when link failure
Voice VLAN optimized	Support Voice VLAN to replace DHCP. In order to use this feature, the Egress port should enable DHCP, the egress port should not be routed port
Support to enable DHCPv6 with MPLS profile	N/A
Support to display the default configuration	Use “show this all” and “show running-configure all” command to display the default configuration
WEB UI optimized	Support to show progress bar when uploading files
Support DHCPv4 server on stacking system	N/A
Support new MIB OID: Mirror Mult-Dest	OID: 1.3.6.1.4.1.27975.3.6
Support multiple devices stacking	Support up to four devices to join one stacking system

2.4 V7.5.3.R

New Features	Specification
Support interface hot split	Support to enable/disable interface split with out reboot
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 EVPN VxLAN Dual home	Support at most 4 devices
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

2.5 V7.5.1.R

New Features	Specification
Resolved Netconf architecture issues	N/A
Support for ED25519 format keys	N/A
Support for IPv6 cross-VNI routing and forwarding	N/A
CPU-TRAFFIC optimization (APP traffic)	N/A
DHCP Server supports static IP binding on ports	N/A
Route- map name length extended from 20 characters to 63 characters	N/A
LLDP enabled on management ports	N/A
S5800 Series,S5850-16T16BS2Q, S3950-4T12S-R,S5850-24S2Q,S5850-24S2C, supports IPv6 BFD	N/A
S8550-32C,S5850-48S8C,S5850-48B8C,S5850-48S6Q-R,S5850-24B4C,S8550- 16Q8C LPM specification optimization & OSPFv3 performance optimization	N/A
COPP whitelist support	N/A

(Stack) 9-slot (Demo)	N/A
ACCESS support for handling tagged packets	N/A
LLDP management address supports VRF	N/A

2.6 V7.4.12.R

New features	Specification
SSH upgraded to OpenSSH 9.8p1 and OpenSSL 1.1.1w	N/A
MLAG supports MSTP	N/A
PVLAN supports tagging	N/A
Stacking supports OSPF BFD	N/A
Netconf supports ACL and Static FDB configuration	N/A
SNMP traps support specifying an IPv6 source address	N/A
MIB supports interface CRC counters	N/A
VXLAN supports DHCP relay functionality after decapsulation	N/A
DHCPv4 relay and DHCPv6 relay support specifying a source address	N/A
L3VPN supports CE-side management	N/A
L3VPN supports multiple Route Reflector (RR) scenarios	N/A
IPv6 RA Guard support added	N/A
HWMonitor reports average latency and timestamps	N/A
Demo-level support for 9-slot stacking	N/A

2.7 V7.4.11.R1

New features	Specification
L4 Port Security	N/A
Support for Scheduled Backup of Configuration Files to TFTP/FTP Server	N/A

Loopback Internal Optimization	N/A
ECN Support in VxLAN Network	N/A
Route-Map Supports Matching Extcommunity-List	N/A
Web Supports Time Range/PoE	N/A
IPSLA Supports MTU Probing	N/A
Stacking Supports NDP and IPv6 Static Routes	N/A
New Image Encryption Feature	N/A
New Device License File Encryption Feature	N/A
Added Passive-Interface All Configuration for OSPF	N/A
Expanded IP/IPv6 Address Capacity on Interface (64 for IPv4, 33 for IPv6)	N/A
Added License Control for NETCONF and RPC	N/A

2.8 V7.4.10.R1

New features	Specification
Stacking support ipv4 BFD link ipv4 static route	N/A
SSH support lock source IP access control	N/A
Support ND Snooping (S8550-32C, S5850-48S8C, S5850-48B8C, S5850-48S6Q-R and the -DC,-PE versions)	N/A
ACE support Description	N/A
Support PTP MIB	N/A
BGP IPv6 VRF support for aggregated routes	N/A
SNMP modify the source port number support SNMPv3	N/A
PBR support IPv6	N/A

2.9 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 OSPFv3 co-work with IPv6 BFD	Support to trigger OSPFv3 status switch by monitoring IPv6 BFD session status. This feature helps the device to achieve high reliability OSPFv3 network.
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 the speed of all S8550-32C interfaces turn down to 40G	Note: in previous versions, system only supports 16 interfaces in middle of the front panel (interface 9 - 24) to turn down to 40G
Support 100G speed for part of interfaces on S8550-16Q8C	Support 100G on interface 9 ~ 16
Support inband/outband SSH/SNMP protection for stacking	N/A
Route-map optimize	Support to set description string for route-map

2.10 V7.4.6.R

Bug Fixes Based on Baseline Version

1) IP LSA supports IPv6 and Track
2) Support Per VLAN configure black hole MAC
3) SNMPv2 supports IPv6 access
4) L2protocol Tunnel supports CDP/VTP
5) Logging server supports specifying IPv6 address and port
6) IPRAN profile renamed to MPLS profile
7) arp broadcast suppression exception (command line causes customer misunderstanding, optimize display)
8) ldp processes crash
9) CPU tx packets cannot be forwarded under special cases

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 MAC_ADDR |)	Use this command to clear sticky port-security mac address table.
	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 |	Use the "ip source guard mode" command to switch between global and

	global)	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.R2

Original format	New format	Remark

show this	show this (all |)	show configurations including defaults
show running-config	show running-config (all |)	show configurations including defaults
-	voice vlan set dscp to DSCP no voice vlan set dscp	Use this command to set DSCP for VOICE packet.
-	voice vlan replace-dscp no voice vlan replace-dscp	Use this command to enable VOICE VLAN replace-dscp on port.
-	ipv6-group NAME (vrf WORD |) (load-share |) no ipv6-group NAME	Use this command to set the ipv6-group. Use the no form of this command to delete the ipv6-group.

3.4 V7.5.3.R

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 <0-7>	Use this command to configure PFC Xoff/Xon threshold for a physical port in absolute value mode. To unset port pfc threshold, use 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	Macsec optimized and command update
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	**Removed** - This command has been removed in this release.	
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 cak simple CAK	macsec cipher-suite (gcm-aes-128 | gcm-aes-256) macsec cipher-suite (gcm-aes-xpn-128 | gcm-aes-xpn-256) no macsec cipher-suite	
mka psk ckn CKN cak simple CAK no mka psk	mka cak-mode static ckn CKN cak CAK no mka cak-mode static	
show mka (default-policy | policy (NAME |))	show mac-security-profile configuration (name NAME |)	
-	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.
-	show resource overlay evpn-	Use this command to display the overlay evpn-

	multihome	multihome resource information.

3.5 V7.4.11.R1

Original format	New format	Remark
-	-	BGP view: neighbor xxx as-origination-interval <0-600>
-	-	IPSLA view: date-size <0-9172>
-	-	IPSLA view: set-df (IPv4 only)
-	-	New ftp server acl command
-	-	OSPF view: Added passive-interface all / no passive-interface all
-	-	Removed loopback port and loopback port mac-address swap commands
-	-	Overlay view: Added command remote-vtep <1-65535> encapsulation-ecn-strategy (ecn-copy|map|none) / no remote-vtep <1-65535> encapsulation-ecn-strategy
-	-	Interface NVE view: Added command encapsulation-ecn-strategy (ecn-copy|map|none) / no encapsulation-ecn-strategy
-	-	show overlay remote-vtep display: Added ES field, modified to abbreviated format for show overlay ipv6 remote-vtep and added ES field to show overlay evpn remote-vtep interface
-	-	Globally added ip unreachables to control ICMP port unreachable message response

3.6 V7.4.10.R1

Original format	New format	Remark
-	-	BGP IPv6 address family new command line neighbor XX::XX nexthop carry-link-local, used to control whether to send update messages carry link-local address.
-	-	add a new command line ip mtu check enable/no ip mtu check enable to control whether to send super-interface MTU messages to the CPU for processing, the default is not on the CPU.

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 |) show 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.
-		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> 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 |	ntp server (mgmt-if | vrf NAME |) (HOSTNAME | IP_ADDR) { key KEY_ID |	Support to specify the VRF name for NTP

version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp server (HOSTNAME | SRC_ADDR)	prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR } no ntp server (mgmt-if | vrf NAME |) (HOSTNAME | SRC_ADDR)	
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
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.R2

Item	Earlier Behavior	New Behavior
static ARP trigger EVPN route	NOT support static ARP trigger EVPN route	Support static ARP trigger EVPN route
Support IPv6 address count limitation	No limitation	Support 3K interface IPv6 address with IPv6 profile and 1K interface IPv6 address with other profiles
BGP default route behavior change	Distribute route 0.0.0.0 with any mask	Distribute route 0.0.0.0/0

4.4 V7.5.3.R

Item	Earlier Behavior	New Behavior
Remove "vxlan gateway-mac" command	Support vxlan gateway-mac	Do not support vxlan gateway-mac
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
Reduce buffer cell when forwarding (Only support on some models. For details, please consult the sales department)	Packet with specified length occupy 2 buffer cells	Packet with specified length occupy 1 buffer cell
Giants frame statistic rule optimized	Packet size large than 1518 or CRC error frames statistic as Giants	Only the packets length large than jumbo frame should statistic as Giants frames

	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	Enable RPC service will not occupy any VTY resource

4.5 V7.4.11.R1

Item	New format	New Behavior
-	-	ERSPAN protocol type changed to 0x88BE
-	-	queues set to default 8-queue mode
-	-	BGP supports zero-delay (no-delay) advertisement of locally originated routes
-	-	hidden command overlay uplink enable controls VXLAN and Geneve with vxlan uplink, and NVGRE with nvgre uplink
-	-	Configuration triggers ARP/ND (supports PBR, OSPF, ISIS)

4.6 V7.4.10.R1

Item	New format	New Behavior
-	-	BGP redistribution of local routes, the local BGP routing protocol face shows the next hop for 0.0.0.0.
-	-	IPv6 BGP can control whether the update message carries link-local address.
-	-	BGP to release the Mars address check (192.0.0.0/8 network segment)
-	-	MTU messages without sending to the CPU by default on the super-interface, forwarded directly.

4.7 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 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 command "show poe summary" output is incorrect.	N/A
The configurable range of the parameter for the multicast command "igmp snooping querier tcn query-interval" are not aligned with operational best practices.	N/A
In some case, PE of L3vpn scene can not access remote private address via the default route of private network	On L3vpn PE, specify the VRF loopback address as source, and specify the remote private address as destination, the packet can not be sent out when it hit the default route
In some case, route switch may lead MPLS ilm entry abnormal and egress port error, which may lead packet loss	When the route flaps, it may lead MPLS ilm abnormal
In VXLAN network, there is a small probably that the MAC address entry is not fully aged bug still exist in the device	In VXLAN network clear and learn MAC address repeatedly may lead MAC address table abnormal
In some case, the private network route include direct connected network can not trigger ARP and it will lead packet loss	The traffic from VPN can not trigger the device to learn the ARP of direct connected hosts.
In some case, Macsec failed to establish session when remote device is produced by other vendor	The remote device sends the mka packets without icv indicator field, lead our device judge it as illegal packed, and failed to establish the session.

5.4 V7.5.3.R

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
Abnormal forwarding behavior of IPv6-PBR	Different interface enables PBR with same match IP, may lead traffic mismatch.
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 nexthop	OSPF status flapping and the underlay route switches 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

5.5 V7.5.1.R

Problem Description	Occurred Condition
IS-IS database anomaly	/
PTP sync packets actual transmission frequency deviates slightly from the configured interval	/
After specific operations, traffic cannot be routed into VXLAN tunnels	/
Device crash when configuring interface descriptions on Debian systems	/
Configuration inconsistency after saving via SSH during incomplete post-boot configuration loading	/
Time-range configuration with special characters causes WEB interface errors	/
Abnormal group-speed behavior in stacking scenarios	/
LACP aggregation failure when adding interfaces with different rates	/
MLAG scenario: LACP system priority configuration does not take effect	/
LSP points to a downed Layer 3 interface	/
Incorrect IS-IS route cost calculation	/
Logs not automatically synced to flash after timeout	/
Stacking scenario: 25G port rate display anomaly in "show interface status"	/
Stack split after SSH login failure	/
DHCP relay unable to enter VXLAN tunnels	/
IS-ISv6 route redistribution exception with OSPFv3	/

5.6 V7.4.12.R

Problem Description	Occurred Condition
The physical address became unreachable after the virtual address was configured	Configuring a virtual address in specific scenarios
BGP BFD failed to establish	Multiple VLAN interfaces in different VRFs were configured with the same IP address
The web interface became unresponsive and could not recover	Deleting a VLAN interface through the web interface
The stack system experienced abnormal splits	Configuring dual-active detection in a stack system
IPv6 neighbors temporarily failed	Receiving specific NA packets

The system crashed with a probability	In EVPN VXLAN scenarios, local and remote devices advertised the same Type 5 route during updates
LDP VC status could not be established	Peer IP was different from the remote router ID
Such traffic was incorrectly dropped	Traffic with Ethertype 0x9009
MLAG negotiation failed to succeed	MLAG flapped
S8550-32C switch connected to servers via front and rear ports during reboot	Server NICs exhibited abnormal UP states during the switch reboot
OSPF cost values were abnormal	OSPF routes were configured
Reflective checks on physical egress ports were unreasonable	Traffic was forwarded to VPLS tunnels
The switch rebooted unexpectedly	Packets were sent to the CPU due to MTU reasons
The device crashed	Receiving large BFD packets

5.7 V7.4.11.R1

Problem Description	Occurred Condition
OSPF linked with BFD fails to trigger ARP learning	-
RPC-API specified with JSON format returns no response	-
Invalid RADIUS authorization privilege, but Telnet still authorizes successfully	-
NETCONF fails to retrieve device configuration in specific configurations	-
Device sporadically prints SDK error log	-
Device becomes unmanaged under continuous SSH attacks	-
Intermittent BGP neighbor disconnections	-
Device crash when using VRF with route-map filtering	-
Unable to specify management port for Telnet to other devices in Debian	-
In stack environment, BFD bound with VRF fails to establish a session with some device	-
DHCP server unable to assign IP addresses in specific scenarios	-
Error when SSH logging into switch with xterm-256color terminal type	-

TACACS server key option invalidates source option	-
Repeated configuration refresh causes stack backup board disconnection	-
BGP neighbor disconnection triggers MLAG neighbor re-establishment	-
Web interface freezes and becomes unrecoverable when editing all ports	-
Physical address of an interface becomes unreachable after configuring a virtual address	-
Stack split occurs due to keepalive timeout after configuring dual-master detection for direct connection	-
Web interface freezes and becomes unrecoverable after deleting VLAN interface	-
BFD session fails to come UP when enabling BGP BFD in specific scenarios	-

5.8 V7.4.10.R1

Problem Description	Occurred Condition
Device received abnormal IGMP Report message, device crash	-
some interfaces of S8550-32C cannot communicate normally after splitting	-
Specific operations under the interface configuration residual	-
FDB drift scenarios with probability of device crash	-
Memory leakage in the execution of specific commands through RPC	-
The address pool range configured by the device as a dhcp server is not fully effective	-
LLDP public node return value does not meet the standard behavior	-
RP port receives duplicate Proposal messages, DP enters the discarding state, and after the RP completes the PA negotiation, the DP initiates another PA negotiation toward the downstream device, causing network oscillation	-
Receiving a specific BGP message, the device disconnects from the BGP connection	-

5.9 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.