Hewlett Packard Enterprise

HPE 5710-CMW710-R6710P03 Release Notes

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 6710P03. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE 5710-CMW710-R671P03 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 6710P03

Note: You can see the version number with the **display version** command in any view. Please see Note①.

Version history

IMPORTANT:

The software feature changes listed in the version history table for each version are not complete. To obtain complete information about all software feature changes in each version, see the *Software Feature Changes* document for this release notes.

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
5710-CMW710-R6710P03	5710-CMW710-R6710	2023-08-01	Release version	Added features. • New feature: DRNI configuraton • New feature: Generating a log message to display product version numbers before and after a software upgrade
5710-CMW710-R6710	5710-CMW710-E6702	2022-12-28	Release version	Added features. • New features: Layer 2—LAN switching features • New features: Layer 3—IP services features • New features: Layer 3—IP routing features • New features: IP multicast features • New features: ACL and QoS features • New features: Security features • New features: High availability features • New features: Network management and monitoring features • New features: Telemetry

Version number	Last version	Release Date	Release type	Remarks
				features • New features: OpenFlow features • New features: VXLAN features • New features: Intelligent lossless network features • New features: M-LAG support for DRNI commands • New feature: FEC mode • New feature: Displaying ND entry statistics • New feature: User IP address conflict SNMP notifications for ARP • New feature: Interface alarm functions • New feature: Advertising only the global unicast address in the NEXT_HOP attribute • New feature: IPv6 duplicate detection on duplicate addresses • New feature: BGP route re-origination • New feature: Establishing neighbors through the secondary IP address of an interface Modified features. • Modified feature: IPv6 routes with prefixes longer than 64 bits • Modified feature: Match criteria in a traffic class • Modified feature: Associating a traffic behavior with a traffic class • Modified feature: Displaying the running configuration • Modified feature: Displaying the contents of the configuration file for the next system startup • Modified feature: Optimized display of BGP BMP server information • Modified feature: Disabling BGP session establishment with peers and peer groups • Modified feature: Optimizations to VXLAN command output • Modified feature: Sharing of VSI interfaces among VSIs • Modified feature: Enabling

Version number	Last version	Release Date	Release type	Remarks
				L2TP for the specified protocol • Modified feature: Creating a local site • Modified feature: Enabling link flapping protection on an interface • Modified feature: AAA methods in an ISP domain • Modified feature: Setting the 802.1X periodic reauthentication timer • Modified feature: Setting the periodic MAC reauthentication timer • Modified feature: Creating an SNMPv3 user • Modified feature: Displaying local public keys • Modified feature: Flow-mirroring traffic to an interface • Modified feature: Disabling the device from learning the source MAC addresses of Layer 2 protocol packets • Modified feature: Specifying multiple VLAN IDs for VLAN name TLVs • Modified feature: Applying a QoS policy to an interface • Modified feature: Configuring MAC address borrowing • Modified feature: Configuring the types of advertisable TLVs on a port • Modified feature: DRNI term changes
5710-CMW710-E6702	5710-CMW710-F2708	2022-04-14	ESS version	Added feature includes: • New feature: Specifying a security enhanced level • New feature: Private VSI Modified feature includes: • Modified feature: Configuring the global priority trust mode for VXLAN packets • Modified feature: Configuring MAC authentication • Modified feature: Disabling BGP from flushing all routes to the routing table • Modified feature: Support for HMAC-SHA-256 OSPF/OSPFv3 authentication mode • Modified feature: Displaying

Version number	Last version	Release Date	Release type	Remarks
				the hash keys used for link aggregation load sharing
5710-CMW710-F2708	5710-CMW710-R2702	2020-12-14	Feature version	Added feature includes: • PTP
5710-CMW710-R2702	5710-CMW710-R2612P05	2019-06-12	Release version	Added feature includes: • New features: Fundamentals features • New features: Virtual technologies features • New features: Layer 2-LAN switching features • New features: Layer 3-IP services features • New features: Layer 3-IP routing features • New features: IP multicast features • New features: ACL and QoS features • New features: Security features • New features: High availability features • New features: Network management and monitoring features • New features: Telemetry features • New features: FC and FCoE features • New features: OpenFlow features • New features: VXLAN features Modified feature includes: • Modified feature: Using an encrypted configuration file to roll back configuration • Modified feature: Support for encrypted configuration files for configuration comparison • Modified feature: Software patching by using issu commands • Modified feature: Automatic configuration • Modified feature: Collision handling in BFD MAD • Modified feature: Processing after the link mode of an Ethernet interface is switched • Modified feature: Configuring MAC-to-VLAN entries • Modified feature: Configuring the advertisable TLVs

Version number	Last version	Release Date	Release type	Remarks
				• Modified feature: Specifying the management address advertised in global management address TLV advertisement setting • Modified feature: Per-packet load sharing mode of aggregation groups • Modified feature: Configuring aging timer for dynamic ARP entries • Modified feature: Enabling ARP snooping • Modified feature: Displaying ARP snooping entries • Modified feature: Clearing ARP snooping entries • Modified feature: Configuring DHCP snooping handling strategy for Option 82 in request messages • Modified feature: Displaying and maintaining ND snooping entries in VLANs • Modified command: display ipv6 nd snooping count • Modified feature: Link state change suppression on an interface • Modified feature: Setting the global aging timer for ND entries in stale state • Modified feature: Setting the interface-specific aging timer for ND entries in stale state • Modified feature: Setting the interface MTU for IPv6 packets • Modified feature: Configuring OSPF area authentication • Modified feature: Configuring OSPF interface authentication • Modified feature: Configuring a virtual link • Modified feature: Displaying IS-IS LSP log information • Modified feature: Clearing IS-IS LSP log information • Modified feature: Displaying detailed BGP routing information • Modified feature: Applying a routing policy to routes outgoing to a peer or peer group • Modified feature: Specifying

Version number	Last version	Release Date	Release type	Remarks
				an ACL • Modified feature: Defining an ACL match criterion in a traffic class of a QoS policy • Modified feature: Applying a QoS policy globally • Modified feature: Configuring a test profile for RADIUS server status detection • Modified feature: RADIUS server quiet timer • Modified feature: Specifying the source IP address for outgoing RADIUS packets • Modified feature: Specifying the source IP address for outgoing HWTACACS packets • Modified feature: Including user IP addresses in MAC authentication requests • Modified feature: Configuring MAC-based MAC authentication user accounts • Modified feature: Handling new MAC access attempts in a VLAN after port security's MAC address limit for that VLAN is reached • Modified feature: Port security NTK feature • Modified feature: Password handling manners with password control enabled globally • Modified feature: Displaying statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping • Modified feature: Displaying statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping • Modified feature: Enabling a VPN instance to replicate routes from the public network or other VPN instances • Modified feature: Setting the maximum number of active routes in a VPN instance • Modified feature: MAC authentication VLAN mode • Modified feature: Port security MAC move • Modified feature: RSA key

Version number	Last version	Release Date	Release type	Remarks
				modulus length • Modified feature: Key modulus length of the RSA key pair used for certificate request in a PKI domain • Modified feature: Configuring the ECDSA signature authentication method in an IKE proposal • Modified feature: Specifying the DH group used for key negotiation in IKE phase 1 • Modified feature: Keyboard-interactive authentication support for SSH users • Modified feature: Displaying IPv4 source guard bindings • Modified feature: Displaying IPv6 source guard bindings • Modified feature: Configuring ARP attack detection logging • Modified feature: Changing the local discriminator of the BFD session for detecting the local interface state • Modified feature: Creating a BFD session for detecting the local interface state • Modified feature: Setting the minimum interval for receiving BFD echo packets • Modified feature: Support for specific BFD commands in VSI interface view • Modified feature: Setting the length of ICMP or ICMPv6 echo requests for the ping operation • Modified feature: Associating Track with application modules • Modified feature: Configuring an interface event for a CLI-defined EAA monitor policy • Modified feature: Configuring an EAA monitor policy by using Tcl • Modified feature: Specifying a source interface for NTP messages • Modified feature: Configuring flow sampling of sFlow • Modified feature: Configuring counter sampling of sFlow • Modified feature: Specifying the role of the device in the

Version number	Last version	Release Date	Release type	Remarks
				VCF fabric • Modified feature: IRF master election during automated VCF fabric deployment • Modified feature: Shutting down an interface by using OpenFlow • Modified feature: Frame match criteria of VXLAN Ethernet service instances • Modified feature: Testing the reachability of remote VMs in VXLANs • Modified feature: Enabling packet statistics for automatically created VXLAN tunnels • Modified feature: Setting the maximum bandwidth for an AC • Modified feature: PW redundancy Deleted feature includes: • Deleted feature:Logging NETCONF row operations Fixed bug.
5710-CMW710-R2612P05	5710-CMW710-R2612P03	2019-03-18	Release version	None.
5710-CMW710-R2612P03	5710-CMW710-R2612P01	2018-10-24	Release version	Added feature includes: • New feature: Default VXLAN decapsulation Modified feature includes: • Modified feature: Setting the maximum bandwidth for a VSI • Modified feature: Setting the broadcast, multicast, or unknown unicast restraint bandwidth for a VSI • Modified feature: Configuring a traffic policing action in a traffic behavior Fix bugs.
5710-CMW710-R2612P01	5710-CMW710-R2612	2018-08-24	Release version	Added feature includes: • New feature: FCoE overview • New feature: FCoE configuration guidelines • New feature: Configuring VFC interfaces • New feature: Enabling FCoE • New feature: Configuring VSANs • New feature: Building a fabric • New feature: Configuring FC

Version number	Last version	Release Date	Release type	Remarks
				routing and forwarding • New feature: Configuring FC zones • New feature: Configuring NPV • New feature: Configuring FIP snooping • New feature: Configuring port security • New feature: Configuring FCS • New feature: Configuring FDMI • New feature: Configuring FC ping • New feature: Configuring FC tracert • New feature: Configuring DCBX • New feature: Configuring the DHCP relay agent to forward DHCP replies based on MAC address table Modified feature includes： • Modified feature: Configuring the types of advertisable TLVs on a Layer 2 Ethernet interface • Modified feature: Displaying local LLDP information • Modified feature: Associating a traffic behavior with a traffic class in a QoS policy Fix bugs.
5710-CMW710-R2612	5710-CMW710-R2611	2018-06-01	Release version	Added feature includes: • New feature: Preprovisioning • New feature: Setting the action that drops matching packets when all next hops specified on an IPv4 or IPv6 policy node are invalid • New feature: Load sharing mode for tunneled traffic on aggregate links Fix bugs.
5710-CMW710-R2611	First release	2018-04-27	Release version	None

Hardware and software compatibility matrix

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	HPE 5710 Series
Hardware platform	5710 48SFP+ 6QS+/2QS28 Switch JL585A 5710 48XGT 6QS+/2QS28 Switch JL586A 5710 24SFP+ 6QS+/2QS28 Switch JL587A 5710 24XGT 6QS+/2QS28 Switch JL689A
Memory	4GB
Flash	1GB
Boot ROM version	Version 241 or higher (Note: Perform the command **display version** command in any view to view the version information. Please see Note ②)
Software images and their MD5 checksums	5710-CMW710-R6710P03.ipe: 39461cb465f9e9ae4076ceeef9f5dfb2
iMC version	iMC EAD 7.3 (E0604) iMC EIA 7.3 (E0604P01) iMC MVM 7.3 (E0506) iMC NTA 7.3 (E0506P03) iMC PLAT 7.3 (E0703) iMC QoSM 7.3 (E0504) iMC RAM 7.3 (E0502) iMC UBA 7.3 (E0506P03) iMC VFM 7.3 (E0505P01)
iNode version	iNode PC 7.3(E0538)
VCF Controller version	E2187 E2180P11
Web version	None
OAA version	None

To display version information for the system software and Boot ROM of 5710:

```
<HPE>display version
<HPE>dis version
HPE Comware Software, Version 7.1.070, Release 6710P03         ------- Note①
Copyright (c) 2010-2023 Hewlett Packard Enterprise Development LP
HPE 5710 48SFP+ 6QS+/2QS28 Switch uptime is 0 weeks, 0 days, 1 hour, 0 minutes
Last reboot reason : Auto Update reboot

Boot image: flash:/5710-cmw710-boot-r6710p03.bin
Boot image version: 7.1.070, Release 6710P03
  Compiled May 05 2023 11:00:00
System image: flash:/5710-cmw710-system-r6710p03.bin
System image version: 7.1.070, Release 6710P03
```

```
  Compiled May 05 2023 11:00:00


Slot 1:
Uptime is 0 weeks,0 days,1 hour,0 minutes
5710 48SFP+ 6QS+/2QS28 Switch with 1 RMI XLP208 Processor
BOARD TYPE:         5710 48SFP+ 6QS+/2QS28 Switch
DRAM:               4096M bytes
FLASH:              1024M bytes
PCB 1 Version:      VER.B
PCB 2 Version:      VER.A
FPGA Version:       NONE
Bootrom Version:    238                                    ------ Note②
CPLD 1 Version:     001
CPLD 2 Version:     002
CPLD 3 Version:     001
Release Version:    HPE 5710 48SFP+ 6QS+/2QS28 Switch-6710P03
Patch Version:      None
Reboot Cause:       AutoUpdateReboot
[SubSlot 0] 48SFP Plus+6QSFP Plus/2QSFP28
<HPE>
```

ISSU compatibility list

Table 3 ISSU compatibility list

Current version	Earlier version	ISSU compatibility
5710-CMW710-R6710P03	5710-CMW710-R6710	Yes
	5710-CMW710-E6702	Yes
	5710-CMW710-F2708	No
	5710-CMW710-R2702	No
	5710-CMW710-R2612P05	No
	5710-CMW710-R2612P03	No
	5710-CMW710-R2612P01	No
	5710-CMW710-R2612	No
	5710-CMW710-R2611	No

Upgrading restrictions and guidelines

Before performing a software upgrade, it is important to refer to the *Software Feature Changes* document for any feature changes in the new version. Also check the most recent version of the related documents (see”Related documentation”) available on the HPE website for more information about feature configuration and commands.

Hardware feature updates

R6710P03

None.

R6710

None.

E6702

None.

F2708

Supports the following new hardware:

- 100G QSFP28 Optical Transceiver Module (1310nm,40km,ER4L,WDM,LC)
- 10G SFP+ Optical Transceiver Module (1270nm,10KM,SMF,BIDI,LC)
- 10G SFP+ Optical Transceiver Module (1330nm,10KM,SMF,BIDI,LC)
- 10G SFP+ Optical Transceiver Module (1270nm,40KM,SMF,BIDI,LC)
- 10G SFP+ Optical Transceiver Module (1330nm,40KM,SMF,BIDI,LC)
- 10G SFP+ Optical Transceiver Module (1490nm,80KM,SMF,BIDI,LC)
- 10G SFP+ Optical Transceiver Module (1550nm,80KM,SMF,BIDI,LC)

R2702

None.

R2612P05

None.

R2612P03

Supports the following new hardware:

- 5710 24XGT 6QS+/2QS28 Switch JL689A

R2612P01

None.

R2612

None.

R2611

First release.

Software feature and command updates

For more information about the software feature and command update history, see HPE 5710-CMW710-R6710P03 Release Notes (Software Feature Changes).

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
5710-CMW710-R6710P03			
New	First release	First release	First release
Modified	First release	First release	First release
5710-CMW710-R6710			
New	None	None	None
Modified	None	None	None
5710-CMW710-E6702			
New	None	None	None
Modified	None	None	None
5710-CMW710-F2708			
New	None	None	None
Modified	None	None	None
5710-CMW710-R2702			
New	None	None	None
Modified	rfc2674-pbridge.mib	P-BRIDGE-MIB	Modified dot1dPortOutboundAccess PriorityTable
5710-CMW710-R2612P05			
New	None	None	None
Modified	None	None	None
5710-CMW710-R2612P03			
New	hh3c-splat-inf.mib	HH3C-LswINF-MIB	Added hh3cifPktBufInDrop hh3cifPktBufEgDrop hh3cifPktBufTable

Item	MIB file	Module	Description
Modified	rfc1213.mib	RFC1213-MIB	Modified sysObjectID
5710-CMW710-R2612P01			
New	None	None	None
Modified	None	None	None
5710-CMW710-R2612			
New	None	None	None
Modified	None	None	None
5710-CMW710-R2611			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R6710P03

- [202306132304] Added the dropped incoming and outgoing packet counts for aggregate interfaces to the ifmgr/statistics table

  Before modification: The ifmgr/statistics table does not provide the dropped incoming and outgoing packet counts for aggregate interfaces.

  After modification: The ifmgr/statistics table provides the dropped incoming and outgoing packet counts for aggregate interfaces.
- [202302250049]Reading the device model, version number, and patch number from MIB objects

  Before modification: The device does not support reading the device model, version number, and patch number from MIB objects.

  After modification: The device supports reading the device model from the hh3cSysProductName MIB object, version number from the hh3cSysProductVersion MIB object, and patch number from the hh3cSysPatchPlatVersion MIB object.

  Remarks: In an IRF fabric, only the device model, version number, and patch number of the master device can be retrieved from MIB objects.
- [202301310408]Modified the restrictions on the source port and monitor port in a mirroring group

  Before modification: The source port and monitor port in a mirroring group cannot both be aggregate interfaces or aggregation member ports.

  After modification: The source port and monitor port in a mirroring group can both be aggregate interfaces or aggregation member ports.
- [202306091868] Assigning an interface to a VLAN on the Web interface

  Before modification: When you log in to the device through the Web interface, you cannot assign an interface to a VLAN.

  After modification: When you log in to the device through the Web interface, you can assign an interface to a VLAN.

Operation changes in R6710

- [202212070921] Added support for NETCONF/gRPC collection of the system power consumption in real time

  Before modification: The chassis and boards data collected through NETCONF/gRPC does not include the total power, residual power, and nominal power data.

  After modification: The chassis and boards data collected through NETCONF/gRPC includes the total power, residual power, and nominal power data.

- [202209051705] IPv6 addresses of BGP peers that exceed 15 characters in the display bgp peer command output are displayed in one line

  Before modification: IPv6 addresses of BGP peers that exceed 15 characters in the **display bgp peer** command output are displayed in two lines.

  After modification: IPv6 addresses of BGP peers that exceed 15 characters in the **display bgp peer** command output are displayed in one line.

- [202208151780] Changed the default state of source MAC address learning for Layer 2 protocol packets

  Before modification: By default, the device learns the source MAC addresses of Layer 2 protocol packets (the **mac-address mac-learning pdu** command is used).

  After modification: By default, the device is disabled from learning the source MAC addresses of Layer 2 protocol packets (the **undo mac-address mac-learning pdu** command is used).

  MAC addresses of the following protocols are involved:

  - BPDUs destined for a MAC address in the range of 0x01-80-c2-00-00-00 to 0x01-80-c2-00-00-0f.
  - GARP PDUs destined for a MAC address in the range of 0x01-80-c2-00-00-20 to 0x01-80-c2-00-00-2f.
  - PVST BPDUs destined for MAC address 0x01-00-0c-cc-cc-cd.

- [202204201853] Optimized the resource alarm log

  Before modification: In the resource alarm log, the Total value equals the sum of the Used value and the Free value.

  After modification: In the resource alarm log, the Total value equals the total number of device resources.

- [202112081667] Modified the maximum value to 9008 for the MTU in VSI view and IP MTU in interface view

  Before modification: The maximum value is 1500 for the MTU in VSI view and IP MTU in interface view.

  After modification: The maximum value is 9008 for the MTU in VSI view and IP MTU in interface view.

- [202204151769]Added support of the CRC error packet alarm function for printing log messages with detailed port numbers

  Before modification: For the CRC error packet alarm function, log messages printed do not contain detailed port numbers.

  After modification: For the CRC error packet alarm function, log messages printed contain detailed port numbers.

- [202205301866]When the parity-error consistency-check log enable, parity-error consistency-check threshold, parity-error unrecoverable log enable, or parity-error unrecoverable reboot command is executed in system view, the configuration is displayed in the configuration file

  Before modification: When the following commands are executed in system view, the configuration is not displayed in the configuration file.

- **parity-error consistency-check log enable**
- **parity-error consistency-check threshold**
- **parity-error unrecoverable log enable**
- **parity-error unrecoverable reboot**

After modification: When the following commands are executed in system view, the configuration is displayed in the configuration file.

- **parity-error consistency-check log enable**
- **parity-error consistency-check threshold**
- **parity-error unrecoverable log enable**
- **parity-error unrecoverable reboot**

- [202112171313] Modified feature: Displaying kernel information upon power cycling of a device

  Before modification: After you execute the reboot command to reboot the device, the device can display kernel-related commands. After you power cycle the device, the device cannot display kernel-related commands.

  After modification: After you power cycle the device, the device cannot display the following kernel-related commands:

  - **display kernel deadloop**: Displays kernel thread deadloop information.
  - **display kernel exception**: Displays kernel thread exception information.
  - **display kernel reboot**: Displays reboot information for the device.
  - **display kernel starvation**: Displays kernel thread starvation information.
- [202201180838] Modified feature: Optimizing downlink interface state switchover time for Monitor Link

  Before modification: In a monitor link group, when the uplink interfaces go down, the state switchover for all downlink interfaces takes a relatively long time.

  After modification: In a monitor link group, when the uplink interfaces go down, the state switchover for all downlink interfaces takes less than 5 seconds.

Operation changes in E6702

None.

Operation changes in F2708

- Added messages to indicate that the FTP and Telnet servers and the SNMPv1 and SNMPv2c versions are insecure because they transmit data in plaintext form. The messages are output when the FTP or Telnet server is enabled or when the SNMP version is set to SNMPv1 or SNMPv2c.

  Before modification: No such messages are output when the FTP or Telnet server is enabled or when the SNMP version is set to SNMPv1 or SNMPv2c.

  After modification: The following messages are output when the FTP or Telnet server is enabled or when the SNMP version is set to SNMPv1 or SNMPv2c:

  - The FTP server is insecure because packets are transmitted in plaintext form.
  - The Telnet server is insecure because packets are transmitted in plaintext form.
  - SNMPv1 and SNMPv2c are insecure because they transmit the community string and data in plaintext form.

Operation changes in R2702

- [201810100437]Added support for using existent and nonexistent policies to filter the BGP routes to be advertised to a peer or peer group.
- [201708150654]Added DHCP support for OVSDB.
- [201809260394]Added the DRNI MIB.
- [201811090674]Added the watchdog timer reset time to the last system reboot information.
- [201901090330]Added CPU model information to the output from the **display version** command.
- [201805220468]Added support for configuring OSPF commands in VSI interface view and disabling a VSI interface from receiving and sending OSPF packets.
- [201904130555]Added SNMP and CLI support for reading the current, voltage, fan direction, and power of a 650 W power supply.
- [201804030211]Added 802.1X MAC address information to the output from the **display mac-address interface** command.
- [201904090672]Added support for inbound and outbound rate limiting for Layer 3 subinterfaces.

Operation changes in R2612P05

- [201902260288]Modified the J Number of 5710 24XGT 6QS+/2QS28 Switch to JL689A and modified the J number of HPE FlexFabric 5710 450W 48V Front-to-Back DC PSU to JL688A.
- [201902220703]Added support for using SNMP to read the vendor part number and product code MIB information of modules

  Before modification: SNMP cannot be used to read the vendor part number and product code MIB information of modules.

  After modification: SNMP can be used to read the vendor part number and product code MIB information of modules.
- [201902220714]Added support for ND flood suppression

  Before modification: The switch does not support ND flood suppression.

  After modification: You can use the **ipv6 nd suppression enable** command to enable ND flood suppression.
- [201902220743]Added support of the **resource-monitor resource ecmpgroup** command for monitoring ECMP group hardware resources in both underlays and overlays

  Before modification: The **resource-monitor resource ecmpgroup** command can monitor only ECMP group hardware resources in underlays.

  After modification: The **resource-monitor resource ecmpgroup** command can monitor ECMP group hardware resources in both underlays and overlays.
- [201902220734]Added support for executing both the **apply service-chain** and **apply default-next-hop** commands in the same PBR policy node view

  Before modification: In the same PBR policy node view, the **apply service-chain** and **apply default-next-hop** commands cannot be both executed.

  After modification: In the same PBR policy node view, the **apply service-chain** and **apply default-next-hop** commands can be both executed.
- [201902220728]Added support for CPU snapshot.
- [201902220719/201812100447]Added support for collecting traffic and bandwidth statistics for aggregate interfaces and aggregate subinterfaces

Before modification: The switch does not collect traffic and bandwidth statistics for aggregate interfaces and aggregate subinterfaces.

After modification: The switch collects traffic and bandwidth statistics for aggregate interfaces and aggregate subinterfaces.

- [201902220718/201809030425]Added support for advertising the IP address of the management Ethernet interface through the management address TLV.

  Before modification: You cannot configure LLDP to advertise the IP address of the management Ethernet interface through the management address TLV.

  After modification: You can configure the management address TLV to carry the IP address of the management Ethernet interface.
- [201902220706]Added support for the **tunnel bfd enable** command in tunnel interface view.
- [201902220690]Added SNMP support for setting the INTERNET community attribute for BGP routes

  Before modification: You cannot issue the **apply community internet** *aa:nn* command through SNMP.

  After modification: You can issue the **apply community internet** *aa:nn* command through SNMP.
- [201902220685]Increased the maximum number of PBR policies that can be configured on a device to 1024

  Before modification: The maximum number of PBR policies that can be configured on a device is 50.

  After modification: The maximum number of PBR policies that can be configured on a device is 1024.

Operation changes in R2612P03

- Added support for using NETCONF to configure the **aggregate** command to create a summary route in the BGP routing table.

  Before modification: NETCONF cannot be used to configure the **aggregate** command to create a summary route in the BGP routing table.

  After modification: NETCONF can be used to configure the **aggregate** command to create a summary route in the BGP routing table.
- Added support for using NETCONF to configure the AS path attribute of a routing policy.

  Before modification: NETCONF cannot be used to configure the AS path attribute of a routing policy.

  After modification: NETCONF can be used to configure the AS path attribute of a routing policy.
- Added support for using NETCONF to apply a routing policy to routes of the specified network segment.

  Before modification: NETCONF cannot be used to apply a routing policy to routes of the specified network segment.

  After modification: NETCONF can be used to configure the **network** *ipv4-address* [*mask-length* | *mask*] [**route-policy** *route-policy-name*] command to apply a routing policy to routes of the specified network segment.
- Added the **Vendor Part Number** field to the **display transceiver interface** command output.

  Before modification: The **display transceiver interface** command output does not support the **Vendor Part Number** field.

  After modification: The **display transceiver interface** command output supports the **Vendor Part Number** field.

- Added support for using NETCONF to assign a preferred value to routes received from a peer or peer group.

  Before modification: NETCONF cannot be used to assign a preferred value to routes received from a peer or peer group.

  After modification: NETCONF can be used to configure the **peer** { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value** *value* command to assign a preferred value to routes received from a peer or peer group.
- Modified the bandwidth value range for traffic of an AC.

  Before modification: The bandwidth value range for traffic of an AC is 64 to 4194303 kbps.

  After modification: The bandwidth value range for traffic of an AC is 64 to 167772159 kbps.
- Modified the broadcast, multicast, or unknown unicast restraint bandwidth for a VSI.

  Before modification: The broadcast, multicast, or unknown unicast restraint bandwidth value range for a VSI is 0 and 64 to 4194303 kbps.

  After modification: The broadcast, multicast, or unknown unicast restraint bandwidth value range for a VSI is 0 and 64 to 167772159 kbps.
- Modified the maximum value for the CIR and PIR parameters in the **car** command to 4294967288 kpps.

  Before modification: The maximum value for the CIR and PIR parameters in the **car** command in traffic behavior view is 160000000 kbps.

  After modification: The maximum value for the CIR and PIR parameters in the **car** command in traffic behavior view is 4294967288 kpps.
- Modified the maximum ARP packet processing rate to 1000 pps.

  Before modification: The maximum ARP packet processing rate is 1800 pps.

  After modification: The maximum ARP packet processing rate is 1000 pps.
- No error information is returned when the **tunnel vpn-instance** command is executed in tunnel view.

  Before modification: When the **tunnel vpn-instance** *vpn-instance-name* command is executed in tunnel view, the system prompts that the command is not supported.

  After modification: When the **tunnel vpn-instance** *vpn-instance-name* command is executed in tunnel view, no error information is returned.
- Added support for using NETCONF to configure the **bestroute igp-metric-ignore** command

  Before modification: NETCONF cannot be used to configure the **bestroute igp-metric-ignore** command.

  After modification: NETCONF can be used to configure the **bestroute igp-metric-ignore** command.

Operation changes in R2612P01

- Added support for FCoE and DCBX

  Before modification: FCoE and DCBX are not supported.

  After modification: FCoE and DCBX are supported.
- Added support for configuring the user-defined device name as **role name-full IP address** in automated VCF fabric deployment

  Before modification: When the device is automatically configured through automated VCF fabric underlay deployment, the device name cannot be configured on Director. The device name is fixed in the **role name-last two fields of IP address** format, for example, **leaf-56.101**.

After modification: When the device is automatically configured through automated VCF fabric underlay deployment, the device name can be configured in the **role name-full IP address** format on Director, for example, **leaf-10.10.56.101**.

- By default, the system does not allocate ACL slice resources to IPv6 and allocates ACL slice resources to IPv6 only after IPv6 is configured, and the system does not allocate ACL slice resources to Layer 3 interfaces

  Before modification: By default, the system allocates two ACL slice resources to IPv6 and two ACL slice resources to Layer 3 interfaces.

  After modification: By default, the system does not allocate ACL slice resources to IPv6 and allocates ACL slice resources to IPv6 only after IPv6 is configured, and the system does not allocate ACL slice resources to Layer 3 interfaces.

Operation changes in R2612

- Added support for packet statistics of VSI interfaces to the MIB

  Before modification: The MIB does not provide packet statistics of VSI interfaces.

  After modification: The MIB provides packet statistics of VSI interfaces.

- Modified the sequence number assignment rule for controller connections

  Before modification: The switch is assigned the same sequence number each time it sets up a connection to the controller.

  After modification: The switch is assigned a different sequence number each time it sets up a connection to the controller.

- Added support for holding the connection to the master controller on the same IRF member switch after an IRF master/subordinate switchover

  Before modification: After an IRF master/subordinate switchover, an IRF member switch is randomly selected to establish the connection to the master controller.

  After modification: After an IRF master/subordinate switchover, the connection to the master controller is held on the same IRF member switch.

- Removed conflicts between the multicast VXLAN tunnel flood proxy feature and the ARP flood suppression feature

  Before modification: When both the multicast VXLAN tunnel flood proxy feature and the ARP flood suppression feature are enabled, the switch cannot operate correctly.

  After modification: If the **vxlan tunnel flooding-proxy** command is not executed, ARP flood suppression is enabled on VSIs. If the **vxlan tunnel flooding-proxy** command is executed, ARP flood suppression is disabled on VSIs.

- Increased the maximum number of ACs mapped to a VSI

  Before modification: A maximum of 256 ACs can be mapped to a VSI.

  After modification: A maximum of 1024 ACs can be mapped to a VSI.

- Added support for OVSDB controller-issued static routes with VSI interfaces as outgoing interfaces.

  Before modification: The switch does not accept OVSDB controller-issued static routes with VSI interfaces as outgoing interfaces.

  After modification: The switch accepts OVSDB controller-issued static routes with VSI interfaces as outgoing interfaces.

- Only one ACL resource is used by multiple users performing MAC authentication

  Before modification: When multiple users perform MAC authentication, multiple ACL resources are used.

  After modification: When multiple users perform MAC authentication, only one ACL resource is used.

- CPU cores monitor each other

  Before modification: CPU cores cannot monitor each other.

  After modification: CPU cores can monitor each other. If a CPU core fails because of deadloop, the device automatically reboots.

Operation changes in R2611

First release.

Restrictions and cautions

When the highest-numbered six QSFP+ interfaces on a 5710 switch are used as 40-GE interfaces and configured as IRF physical interfaces, follow these restrictions and guidelines:

- As a best practice, when both ends use one of the first four QSFP+ interface or use one of the last two QSFP+ interfaces, you can use transceiver modules, fiber cables, or copper cables to connect the IRF physical interfaces.
- When one end uses one of the first four QSFP+ interfaces and the other end uses one of the last two QSFP+ interfaces, use transceiver modules or fiber cables to connect IRF physical interfaces.

Open problems and workarounds

202307130980

- Symptom: ARP and ND entries of DRNI extra VLANs cannot be synchronized over the peer link.
- Condition: This symptom might occur if an DRNI member device reboots or its peer-link interface flaps.
- Workaround: None.

List of resolved problems

Resolved problems in R6710P03

202306080897

- Symptom: The device generates message **Failed to save license data to the primary license storage area** at intervals of 24 hours.
- Condition: This symptom occurs when the system fails to read and write the license storage area because of flash memory failure.
- Remarks：None.

202305291927

- Symptom: API Device/Base cannot be read on Postman.
- Condition: This symptom might occur when you use Postman to retrieve the Device/Base node.
- Remarks: None.

202305100224

- Symptom: Protocol packets are dropped in an EVPN VXLAN-DCI network.

- Condition: This symptom occurs if the TTL of the protocol packets is 1.
- Remarks: None.

202211031872

- Symptom: During the ISSU loading process, one IRF member device experiences packet loss for approximately 18 seconds.
- Condition: This symptom occurs if EVPN VXLAN is configured on IRF member devices, a subordinate member device is restarted, and Layer 3 VXLAN traffic by default matches a blackhole route.
- Remarks: None.

202303131038

- Symptom：In the output from the display ipv6 interface command, the IPv6 address, interface name, and VPN fields are displayed on different lines, which should be displayed on the same line.
- Condition：This symptom occurs if you execute the display ipv6 interface command.
- Remarks：None.

202305221758

- Symptom：When the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface, the outgoing VXLAN packets carry VLAN tag 4095 unexpectedly. As a result, the peer cannot learn ARP entries.
- Condition：This symptom occurs if the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface.
- Remarks：None.

202305300007

- Symptom：Creation of a VSI interface, Layer 3 subinterface, or Layer 3 aggregate subinterface might fail.
- Condition：This symptom occurs if a VSI interface, Layer 3 subinterface, or Layer 3 aggregate subinterface is created.
- Remarks：None.

202304240579

- Symptom: Isolation of aggregation member ports no longer takes effect on a DR interface, and the traffic is forwarded between the aggregation member ports.
- Condition: This symptom occurs if the following operations are performed:
  a. Shut down all aggregation member ports of the IPP and DR interfaces, save the configuration, and reboot the device.
  b. Bring up the aggregation member ports of the IPP.
  c. After half of the DRNI restoration delay elapses, bring up the aggregation member ports of the DR interfaces.
- Remarks: None.

202209230460

- Symptom: In gRPC dial-in mode, some sampling paths cannot collect data and the data is collected by other sampling paths.
- Condition: This symptom might occur if you configure multiple sampling paths in gRPC dial-in mode.
- Remarks: None.

202211140499

- Symptom: OSPF BFD flaps repeatedly.
- Condition: This symptom occurs if you use borrowed loopback interface addresses to establish OSPF neighbor relationship, configure BFD for OSPF, and then reboot the device.
- Remarks：None.

202302150003

- Symptom: The log file **fabric.log** generated by VCF fabric exhausts the memory.
- Condition: This symptom occurs if the automated deployment scenario of VCF fabric runs for a long period of time or interfaces flap.
- Remarks：None.

202305110216

- Symptom: On a multicast VXLAN network, multicast traffic cannot be forwarded.
- Condition: This symptom occurs if the device starts with the factory defaults and then you configure multicast VXLAN in the following order: first configure tunnels and VSIs, and then configure multicast.
- Remarks：None.

202304171574

- Symptom: The switch cannot obtain an IPv6 address after it is rebooted, and IPv6 automatic deployment fails.
- Condition: This symptom occurs if the controller deploys the configuration to change the hardware resource mode during automatic deployment and the controller does not assign a fixed IPv6 address.
- Remarks：None.

202305081426

- Symptom: In an EVPN or VXLAN distributed gateway network, when the device receives a tunneled packet with a source IP address the same as a VSI interface address, the device will reply with a gratuitous ARP response, which can lead to high CPU usage.
- Condition: This symptom might occur if the distributed gateways perform ARP probing in response to traffic.
- Remarks：None.

202306100168

- Symptom: A device attached to an DRNI system with dual-active VLAN gateways configured cannot learn ARP information about a peer.
- Condition: This symptom occurs if a device attached to an DRNI system with dual-active VLAN gateways sends an ARP request to obtain the ARP information about a peer.
- Remarks：None.

202305120926

- Symptom: The device gets stuck after a controller deploys the default action to interfaces on the device.
- Condition: This symptom occurs if the device has port security settings and the controller uses multiple sessions to deploy the default action.
- Remarks：None.

202304250098

- Symptom: After the **peer advertise vpn-reoriginate ibgp** command is executed, the local device removes private AS numbers (in the range of 65512 to 65534) from routes before advertising those routes to the specified peers. This operation affects the results of optimal route selection on the peers. When you execute the **display bgp update-group l2vpn evpn** command to view the update group information for the specified peers, the command output displays **Public-AS-Only: Yes**.
- Condition: This symptom occurs if you execute the **peer advertise vpn-reoriginate ibgp** command. This command enables the device to remove private AS numbers (in the range of 65512 to 65534) from routes before the device advertises those routes to the specified peers.
- Remarks：None.

202305100217

- Symptom: When an endpoint sends an RARP message, the route used for forwarding traffic to the endpoint flaps, and traffic loss occurs.
- Condition: This symptom occurs if an endpoint dualhomed or singlhomed to an EVPN DRNI system sends an RARP packet.
- Remarks：None.

202303160020

- Symptom: When a DHCP user comes online, the DHCP process is closed abnormally.
- Condition: This symptom might occur if the following conditions exist:
  a. The DHCP user comes online through interface 1 and two IP addresses (for example, IP address A and IP address B) are obtained.
  b. The DHCP user later comes online through interface 2 and IP address A is obtained.
  c. The clientinfo entries on the DHCP relay device are reset.

202306060566

- Symptom: After OSPF establishes a neighbor relationship with a neighboring device, the neighbor cannot learn the default route advertised by the local device.
- Condition: This symptom might occur if you create OSPF view without associating any interfaces and then execute the **nssa default-route-advertise** command.
- Remarks：None.

202305200093

- Symptom: The device is disconnected from the controller when a patch is installed from the controller.
- Condition: This symptom occurs if you install a patch from the controller and restart the xmlcfgd process when the patch is installed.
- Remarks：None.

202301120578

- Symptom: After an incremental patch is uninstalled, the **display boot-loader** command does not display information about a non-incremental patch.
- Condition: This symptom occurs if both an incremental patch and a non-incremental patch are installed.
- Remarks：None.

202206071105

- Symptom: When you configure an **s-vid** (outer VLAN IDs) match criterion for a VPLS Ethernet service instance, you can only specify a single VLAN ID and cannot specify a VLAN ID range.

- condition: This symptom occurs when you configure a packet match criterion for an Ethernet service instance of a VPLS network.

202305220011

- Symptom: IP address conflicts occur between four leaf devices because of inconsistent ARP and MAC information, and the CPU usage of the leaf devices reaches 70%.
- Condition: This symptom occurs if the following conditions exist:
  - With ARP proxy enabled, a probe packet is sent when a remote ARP rule for EVPN is withdrawn.
  - A probe packet is sent if a remote ARP rule overwrites a local ARP entry.
- Remarks：None.

Resolved problems in R6710

202208241285

- Symptom: A QoS policy applied to a control plane cannot filter the protocol packets to the control plane
- Condition: This symptom occurs when you apply a QoS policy to a control plane to filter protocol packets.
- Remarks: None.

202211010383

- Symptom: When a client-oriented MACsec connection is established between an Aruba device and HPE switch, the MACsec protocol cannot come up, and the connection cannot be established correctly.
- Condition: This symptom occurs if a client-oriented MACsec connection is established between an Aruba device and HPE switch.
- Remarks: None.

202204071026

- Symptom: A QoS policy applied to a VSI takes effect only on traffic forwarded at Layer 2 and does not take effect on traffic forwarded at Layer 3.
- Condition: This symptom occurs if a QoS policy is applied to a VSI.
- Remarks: None.

202211050218

- Symptom: After the BFD MAD configuration is deleted from a VLAN interface, the configuration remains.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on the VLAN interface, and bind the VLAN interface to a VPN instance.
  b. Configure BFD MAD on an aggregate interface. Bind the aggregate interface to the same VPN instance as the VLAN interface.
  c. Delete the BFD MAD configuration from the VLAN interface.
  d. Delete the VLAN interface configured with BFD MAD.
- Remarks: None.

202211050189

- Symptom: After an IRF member device is rebooted, the **display bfd session** command output displays two BFD MAD sessions.

- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on an aggregate interface, and bind the aggregate interface to a VPN instance.
  b. Delete the BFD MAD configuration from the aggregate interface.
  c. Configure BFD MAD on a VLAN interface. Bind the VLAN interface to the same VPN instance as the aggregate interface.
  d. Configure BFD MAD on the aggregate interface again.
  e. Reboot an IRF member device. After the device is rebooted and the IRF fabric is formed again, execute the **display bfd session** command to display the BFD MAD sessions.
- Remarks: None.

202204090439

- Symptom: The console gets stuck after repeated execution of the **port-security enable** or **port-security port-mode** command.
- Condition: This symptom occurs if the **port-security enable** or **port-security port-mode** command is repeatedly executed.
- Remarks: None.

202207121416

- Symptom: IS-IS neighbors are disconnected during an ISSU.
- Condition: This symptom might occur if the device has established IS-IS neighbor relationships and an ISSU is performed to upgrade the software from 27xx to 67xx.
- Remarks: None.

202209120087

- Symptom: A QoS policy that contains multiple class-behavior associations is applied to the outbound direction of the device. When the actions in a class-behavior association are modified, traffic might match another class-behavior association by mistake.
- Condition: This symptom occurs if the following operations are performed:
  a. Apply a QoS policy to multiple interfaces. A behavior contains the counting or CAR action.
  b. Modify the actions in a traffic behavior or match criteria in a traffic class in the QoS policy or another QoS policy. Or, apply the QoS policy again.
- Remarks: None.

202109131526

- Symptom: Untagged packets cannot be forwarded for a local VLAN to a remote VXLAN.
- Condition: This symptom might occur if the device is operating in border mode and forwards untagged packets of a local VLAN over a VXLAN tunnel.
- Remarks: None.

202208311310

- Symptom: IPv6 automated device deployment is interrupted.
- Condition: This symptom might occur if the device performs IPv6 automated device deployment.
- Remarks: None.

202207080423

- Symptom: MAC authentication users flap on an aggregate interface 8 minutes after they come online.

- Condition: This symptom might occur if MAC authentication user offline detection is enabled by default.
- Remarks: None.

202206291177

- Symptom: The device receives NA packets that do not carry the target link-layer address field and does not learn ND entries from the NA packets.
- Condition: This symptom might occur if the device receives unrequested NA packets that do not carry the target link-layer address field.
- Remarks: None.

202206230765

- Symptom: The device reports a permission deny error.
- Condition: This symptom might occur if command authorization is enabled and the **repeat** command is executed for more than 1000 times.
- Remarks: None.

202206060838

- Symptom: In Layer 3 multicast on a cascaded M-LAG network, IGMP packets are looped between M-LAG interfaces.
- Condition: This symptom occurs if an M-LAG interface receives IGMP query packets.
- Remarks: None.

202210250334

- Symptom: The number of free resources in the **display resource-monitor resource nexthoppool1** command output increases all the time, and a resource alarm is triggered
- Condition: This symptom occurs if the switch learns a large number of ARP entries and you execute the **reset arp** command.
- Remarks: None.

202209200820

- Symptom: Memory is leaked.
- Condition: This symptom occurs if you add and delete Layer 3 aggregate subinterfaces.
- Remarks: None.

202201171691

- Symptom: A QoS policy is still in effect after it is removed from a VSI interface.
- Condition: This symptom occurs if you perform the following operations:
  a. Create a QoS policy without class-behavior associations, and apply it to a VSI interface.
  b. Configure a class-behavior association in the QoS policy, and remove the QoS policy from the VSI interface.
- Remarks: None.

202112270288

- Symptom: In an IRF fabric with multichassis aggregation, the memory is exhausted, and the switch reboots when a large number of MAC authentication users come online on an aggregate interface.
- Condition: This symptom occurs if offline detection and reauthentication are enabled.
- Remarks: How many users can cause this problem depends on the size of the memory. In this example, 16000 users come online in four groups at 300 users per second (4000 in each group).

202206010870

- Symptom: In a network with two IRF fabrics, BFD MAD flaps.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable BFD MAD on interfaces in the same VLAN.
  b. Perform a master/subordinate switchover on one IRF fabric.
- Remarks: None.

202204290654

- Symptom: In an IRF fabric with multichassis link aggregation, some of the aggregation member ports cannot forward traffic, causing uneven hashing after member ports are shut down and then brought up.
- Condition: This symptom occurs if the aggregate interface acts as an outgoing interface for a VXLAN tunnel.
- Remarks: None.

202204191568

- Symptom: The convergence time of the Monitor Link down function is long.
- Condition: This symptom occurs when the downlink interfaces in a monitor link group are shut down because an uplink interface goes down.
- Remarks: None.

202204230202

- Symptom: A MAC address move does not trigger an ND move.
- Condition: This symptom might occur in an underlay M-LAG network if the **mac-address mac-move fast-update** command is executed.
- Remarks: None.

202109131526

- Symptom: The device cannot forward untagged packets from a VLAN to a remote VXLAN.
- Condition: This symptom occurs if the device in border mode forwards untagged packets from a VLAN out of a VXLAN tunnel.
- Remarks: None.

202205091696

- Symptom: The reply to an HTTP request on a device carries the server:HTTPD field, which is used to identify the server information. The vulnerability scanners consider that the server field might disclose the server information and result in attacks.
- Condition: This symptom occurs if the device receives HTTP requests.
- Remarks: None.

202205091688

- Symptom: The memory leaks for the routed module.
- Condition: This symptom occurs if you configure a gRPC sensor path to collect route information, and then make routes on the device flap.
- Remarks: None.

202203141354

- Symptom: After the device is rebooted, the detection interval configured for the BFD echo session does not take effect, and is displayed as the default value.
- Condition: This symptom occurs if the following operations are performed on a DRNI network:

a. Configure a static BFD echo session with a detection interval different from that configured for the BFD echo session on an interface. The session can be negotiated as up.
b. Save the configuration, and then reboot the device.

- Remarks: None.

202205171718

- Symptom: When identical static ARP entries are configured on the DR member devices in a DR system, configuration fails on one DR member device.
- Condition: This symptom might occur if identical static ARP entries are configured on the DR member devices in a DR system.
- Remarks: None.

202105150186

- Symptom: After an aggregate interface authenticates a MAC authentication user, an IRF master/subordinate switchover occurs, and the user goes offline 10 minutes later.
- Condition: This symptom occurs if an aggregate interface authenticates a MAC authentication user and an IRF master/subordinate switchover occurs.
- Remarks: None.

202204290651

- Symptom: Layer 3 aggregate subinterfaces do not forward traffic.
- Condition: This symptom might occur if cross-device aggregation is configured in stack deployment and both Layer 3 aggregate subinterfaces and Layer 3 subinterfaces act as equal-cost outgoing interfaces for a VXLAN tunnel.
- Remarks: Shut down and bring up any outgoing interface for the VXLAN tunnel after patch installation.
- Remarks: None.

Resolved problems in E6702

None.

Resolved problems in F2708

202006240947

- Symptom: When you apply a QoS policy, the system prompts that the QoS and ACL resources are insufficient.
- Condition: This symptom occurs if the traffic classifiers of the QoS policy reference both IPv4 and IPv6 ACLs.
- Remarks: None.

202004081619

- Symptom: The device cannot be logged in.
- Condition: This symptom occurs if password control is enabled on the device and the system time change causes the login password to expire.
- Remarks: None.

202006150135

- Symptom: When a 10-GE interface on an 5710 24XGT 6QS+/2QS28 Switch JL689A connects to a peer GE interface, packet loss occurs.
- Condition: This symptom occurs if a 10-GE interface on an 5710 24XGT 6QS+/2QS28 Switch JL689A connects to a peer GE interface.
- Remarks: None.

202008140876

- Symptom: The time in the **display clock** command output is not accurate.
- Condition: This symptom occurs if the following conditions exist:

  The **clock protocol ntp** command is executed to specify NTP for obtaining the time.

  The time difference between the system and the NTP server exceeds 68 years.
- Remarks: None.

202006280209

- Symptom: The number of received packets and the number of sent packets on an interface abnormally increase in the interface statistics.
- Condition: This symptom occurs if a 40-Gbps transceiver module is removed from a 100-GE interface.
- Remarks: None.

202010150963

- Symptom: The **reset packet-drop** command cannot clear the dropped packet statistics for an interface.
- Condition: This symptom occurs if the **reset packet-drop** command is executed to clear the dropped packet statistics when congestion occurs on an interface.
- Remarks: None.

202002251001

- Symptom: No error message is prompted for patch installation failure.
- Condition: This symptom occurs if you log in to the device through Telnet or SSH and the patch installation fails.

202005191016

- Symptom: A 10-GE transceiver module inserted into a 40-GE interface by using a 40-GE to 10-GE adapter fails to transmit optical signals correctly.
- Condition: This symptom occurs if a 10-GE transceiver module is inserted into a 40-GE interface by using a 40-GE to 10-GE adapter.
- Remarks: None.

202005090333

- Symptom: After you configure a PBR policy and enable packet statistics for a Layer 3 Ethernet subinterface, the PBR policy cannot take effect.
- Condition: This symptom might occur if you configure a PBR policy and enable packet statistics for a Layer 3 Ethernet subinterface.
- Remarks: None.

202004300168

- Symptom: For a 40-GE interface manually shut down, a 10-GE transceiver module inserted into this interface by using a 40-GE to 10-GE adapter can transmit optical signal correctly. After the transceiver module is removed and reinstalled in the 40-GE interface, the interface comes up.

- Condition: This symptom occurs when the following operations have been performed:
  a. Execute the **shutdown** command on the 40-GE interface.
  b. Insert a 40-GE to 10-GE adapter into the 40-GE interface.
  c. Insert a 10-GE transceiver module into the adapter and connect the interface to a peer device.
  d. Remove and reinstall the 10-GE transceiver module in the interface.
- Remarks: None.

202004231154/202004240282

- Symptom: In a VRRP group, the device with higher priority is elected as the backup and cannot become the master.
- Condition: This symptom might occur if you continuously modify the device priorities to perform master/backup switchover in the VRRP group (with version VRRPv2 or VRRPv3).
- Remarks: None.

202004290297

- Symptom: The match order of issued PBR policy nodes is incorrect.
- Condition: This symptom might occur if PBR policies are issued to multiple interfaces and the interface (pointing to a next hop in a PBR policy) in an ARP entry has change to another interface.
- Remarks: None.

202004290738

- Symptom: IPv4 or IPv6 Layer 3 VPN traffic is interrupted when the public network routes repeatedly flap on an IRF fabric.
- Condition: This symptom might occur if the following conditions exist:
  - On the IRF fabric, a multichassis aggregate interface acts as the output interface of BGP public network routes.
  - The member ports of the aggregate interface are repeatedly shut down and then brought up.
- Remarks: None.

202001130806

- Symptom: When executing the **irf member renumber** command, the system should output a message indicating that a reboot is required for this command to take effect. However, the system does not output this message.
- Condition: This symptom occurs when the **irf member renumber** command is executed.

201912260195

- Symptom: 10-GE ports on the local device are connected to the breakout interfaces of a 40-GE port on the neighbor device through AOC cables. Packet loss occurs on all the 10-GE ports connected to the breakout interfaces.
- Condition: This symptom occurs if you remove and then insert the AOC cable for one of the 10-GE breakout interfaces on the neighbor device.

202002060416

- Symptom: BFD MAD still remains in Faulty sate on an IRF fabric after the IRF fabric recovers from an IRF split event.
- Condition: This symptom occurs if the following conditions exists:
  a. The IRF fabric contains two member devices and BFD MAD is configured on the IRF fabric.
  b. The IRF fabric splits and then recovers.

202001190271

- Symptom: The telnet operation hangs with a low probability.
- Condition: This symptom might occur if you telnet to the device, and enable command accounting but the accounting server is not available.

201905210848

- Symptom: The link aggregation module cannot process services when the BFD session flaps.
- Condition: This symptom might occur if you configure collaboration between Ethernet link aggregation and BFD.

202002180298

- Symptom: The packet statistics for VLAN interfaces and VSI interfaces are incorrect.
- Condition: This symptom occurs if packet statistics are collected for VLAN interfaces and VSI interfaces.

201912300910

- Symptom: When the automatic configuration feature is used to replace an IRF member device, the IRF member devices not replaced also reboot during the replacement process.
- Condition: This symptom occurs when the automatic configuration feature is used to replace an IRF member device.

201908060060

- Symptom: The help information for the **display interface** command cannot be displayed.
- Condition: This symptom occurs if the **ifmgr** process is restarted.

201912170482

- Symptom: After a reboot, the switch cannot forward VXLAN traffic based on a static route, and a static ARP entry becomes a blackhole entry.
- Condition: This symptom might occur if the following operations are performed on the switch:
  a. Configure a static ARP entry.
  b. Save the running configuration.
  c. Reboot the switch.

201911040571

- Symptom: Failed to create a VSI interface by using the **interface vsi** command.
- Condition: This symptom might occur if the following operations are performed:
  a. Create a service loopback group and assign member ports to the service loopback group.
  b. Create GRE tunnel interfaces.
  c. Create a VSI interface.

201910080448

- Symptom: Transient packet loss occurs on an interface when the **undo packet-filter** command is executed to remove an ACL from the interface.
- Condition: This symptom might occur if the ACL has multiple rules and the action is set to deny in the last rule.

201907290489

- Symptom: The host cannot ping the gateway that has a PBR policy configured.
- Condition: This symptom might occur when you ping the switch (acting as the gateway) configured with a PBR policy from the host.

201906060558

- Symptom: An interface configured with a PBR policy flaps and the PBR policy no longer takes effect when ECMP is configured on the interface.
- Condition: This symptom might occur if ECMP is configured on an interface where a PBR policy is applied.

201905141113/201901070710

- Symptom: Some tunneled packets are lost on the output interface.
- Condition: This symptom occurs when the output interface for tunneled packets changes from a physical interface to an aggregate interface.

201907231134

- Symptom: The session timeout information still exists in the **display dot1x connection** command output after the server deletes the Session-Timeout attribute during an 802.1X reauthentication.
- Condition: This symptom occurs if the server assigns the Session-Timeout attribute to an 802.1X user during the first authentication and then deletes the Session-Timeout attribute during an 802.1X reauthentication.

201907020289

- Symptom: A user fails MAC authentication on an interface if its MAC address has been learned by another interface of the switch.
- Condition: This symptom might occur if a MAC authentication user accesses an interface and its MAC address has been learned by another interface of the switch.

201905210842

- Symptom: Multiple Telnet users exist and cannot be deleted after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Telnet to the switch from multiple terminals.
  b. On each terminal, execute the **telnet 127.0.0.1** command multiple times and press Ctrl + K.
  c. Execute the **display users** command on the switch.

201908010003

- Symptom: The virtual IP addresses of new VRRP groups cannot be pinged after the number of VRRP groups exceeds 512.
- Condition: This symptom might occur if more than 512 VRRP groups are configured.

201908280757

- Symptom: Layer 3 traffic forwarding is interrupted.
- Condition: This symptom might occur after you disable packet statistics for the Layer 3 aggregate subinterface by using the **undo traffic-statistic enable** command.

201905160399

- Symptom: The CPU usage keeps at 100% for a long time after a recursion loop occurs.
- Condition: This symptom might occur if the following conditions exist:
  - The device has two BGP routes, route **1** and route **2**. Route **1** has a primary next hop **a** and a backup next hop **b** (specified by using FRR); route **2** has a primary next hop **b** and a backup next hop **a** (specified by using FRR).
  - Both **a** and **b** are on the same network segment as the destination networks of route **1** and route **2**.

- The interfaces pointing to both **a** and **b** go down within a short period of time. As a result, the device selects the backup next hop for both routes. A recursion loop occurs.

Resolved problems in R2702

201905200485/201901090410

- Symptom: On the IRF fabric, the management address fails to be displayed in the LLDP information received from the neighboring devices.
- Condition: This symptom might occur if the following conditions exist:
  a. VLAN interfaces are created on the IRF fabric and IP addresses are assigned to the interfaces.
  b. An IRF subordinate device reboots.

201812060001

- Symptom: The XMLCFGD process creates a core file unexpectedly.
- Condition: This symptom might occur if a NETCONF connection is established to the device to manage the device and NETCONF is used to reboot the device.

201809290321

- Symptom: On a DRNI network, a device reboots because of memory exhaustion.
- Condition: This symptom might occur if the following conditions exist:
  a. The keepalive timeout timer on the secondary DR member device is set to the maximum value.
  b. A configuration rollback is performed on the primary DR member device to cancel the DRNI configuration and then another configuration rollback is performed to recover the DRNI configuration.

201902010798

- Symptom: A device management user fails to obtain another user role by using the **super** command.
- Condition: This symptom might occur if the device management user logs in to the device after passing HWTACACS authentication and executes the **super** command to obtain another user role.

201904010489

- Symptom: The device fails to forward traffic correctly.
- Condition: This symptom might occur if a loop exists on the device, which causes the ARP table to update repeatedly and then causes FIB table update failure.

201903211294

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the control plane deploys entries that contain unassigned IP addresses to the data plane on a control-/data-plane separated network.

201807190673

- Symptom: The ofcd process fails because of exception.
- Condition: This symptom might occur if the established OpenFlow tunnel is attacked by exception OpenFlow packets in which the length of the protocol header field is 0.

201809110564

- Symptom: The cp process still remains on the device after the connection to the controller is terminated.
- Condition: This symptom might occur if the controller deploys the **save** command through NETCONF to save the running configuration and then terminates the connection to the device.

201811060548

- Symptom: The CPU usage rises rapidly during inter-VPN traffic forwarding.
- Condition: This symptom might occur if BGP redirects direct routes between multiple VPN instances.

201809200079

- Symptom: The RADIUS server fails to assign an authorization VLAN name to a user after the user passes authentication.
- Condition: This symptom might occur if the authorization VLAN name is in the format of \000XXXXX\000.

201904010490

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if ARP entries are deleted when SNMP is walking the ARP table.

201904020841

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if TCP MSS is set on a subinterface and the subinterface is repeatedly deleted and created when SLB traffic is forwarded.

201807300378/201905090714

- Symptom: A memory leak occurs on the SNMP process.
- Condition: This symptom occurs if the following conditions exist:
  a. SNMP notifications for system logs are disabled.
  b. The NMS walks the SYSLOG-MSG-MIB to obtain data.

201811070579

- Symptom: The lauthd process creates a core file unexpectedly.
- Condition: This symptom might occur if the **local-user-export class network guest url b** command is executed consecutively several times.

201811060248

- Symptom: The IMC server forcibly logs out a portal user after the user passes portal authentication.
- Condition: This symptom might occur if the portal authentication server runs IMC PLAT 7.3 and security policy confirmation (such as ACL and VLAN) is deployed on the IMC server.

201810230548/201809120806

- Symptom: A memory leakage occurs on a subordinate device in an IRF fabric.
- Condition: This symptom might occur if portal users that obtain IP addresses through DHCP carries Option 82 or Option 18 when they come online.

201809200058

- Symptom: The Aaad process on an IRF fabric creates a core file unexpectedly.
- Condition: This symptom might occur if the following conditions exist:

- A large number of IPoE users come online through the IRF fabric.
- Master/subordinate switchover repeatedly takes place.
- The AAA process reboots repeatedly.

201812070009/201812061078

- Symptom: Specific UDP packets get lost during forwarding.
- Condition: This symptom might occur if a UDP packet has the following characteristics:
  - The packet is a fragment packet.
  - The packet carries MPLS labels.
  - The third and fourth bytes in the IP header of non-first fragment packets is 0D AF.

201811060034

- Symptom: An IPsec SA is established between the device and the peer device through IKEv2 negotiation and the security protocol is ESP. IPsec protocol packets from the peer device are discarded because the packet length exceeds the port MTU.
- Condition: This symptom might occur if TFC padding is enabled and IPsec packet fragmentation is disabled on the peer device.

201903211236

- Symptom: The CLI of a device in an IRF fabric gets stuck and no commands can be input.
- Condition: This symptom might occur if a large number of tunnels flap and IRF master/subordinate switchover repeatedly takes place.

201902020055

- Symptom: IS-IS neighbor relationship cannot be established.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the network type as P2P and enable IS-IS on an interface.
  b. Reboot the device.

201904020277

- Symptom: ARP entries become blackhole entries, and packets are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Multiple Layer 2 aggregation groups exist in the network, and loops exist in some aggregation groups.
  b. Enable ARP active acknowledgement.
  c. Configure static routes on a Layer 3 interface. Shut down and then bring up the Layer 3 interface, or MAC address moves occur on the Layer 3 interface.

201902020232

- Symptom: The master IRF member device might reboot unexpectedly at a low probability.
- Condition: This symptom occurs if the following operations are performed:
  a. Set a small idle timeout value for TCP connections.
  b. Initiate a large number of TCP connections for services using TCP (for example, BGP and HTTP) on the local end.

201811060022

- Symptom: The memory leaks for the IPFS module.
- Condition: This symptom occurs if the following conditions exist:
  - A large amount of traffic with varying quintuples is forwarded by software.
  - The fast forwarding entries age out.

201902020140

- Symptom: After the TCP client connection is closed, the memory leaks.
- Condition: This symptom occurs if the following operations are performed:
  a. The client sends a large amount of data to the server. The server cannot process so much data, so the server responds with Zero Window.
  b. The client starts the persist timer after receiving Zero Window.
  c. The client actively closes the connection.

201902020187

- Symptom: The CPU usage might be high at a low probability.
- Condition: This symptom occurs if a large number of packets are transmitted when a user logs in through nested Telnet.

201812070478

- Symptom: An interface on a subordinate IRF member device cannot join a voice VLAN again after leaving the voice VLAN.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable LLDP on an interface on a subordinate IRF member device, and configure a voice VLAN on the interface. Connect the interface to a voice device supporting LLDP/CDP.
  b. Establish or disconnect the LLDP neighbor relationship on the subordinate IRF member device.

201811060177

- Symptom: After an IP phone successfully comes online, the gateway cannot ping the IP phone for a period of time.
- Condition: This symptom occurs if the following operations are performed:
  a. Connect an interface to a Cisco IP phone, enable CDP-compatible LLDP on the interface, and assign the IP phone to a voice VLAN.
  b. The interface repeatedly comes up and goes down.

201811060399

- Symptom: A DHCP client cannot obtain an IP address.
- Condition: This symptom occurs if the device acts as a DHCP sever, multiple address pools are configured, and some address pools are configured with address ranges for dynamic allocation by using the **address range** command.

201812060884

- Symptom: The XMLCFGD process exits exceptionally.
- Condition: This symptom occurs if the following operations are performed:
  a. The device acts as a DHCP Sever. In a DHCP address pool, configure more than 13 static IP address bindings.
  b. Use SoapUI to get the data of the DHCP/DHCPServerPoolStatic table.

201810290644

- Symptom: During auto upgrade, the **using tengige** command is mistakenly executed. As a result, the comsh process becomes abnormal, and related interfaces disappear.
- Condition: This symptom occurs because the **using tengige** command is mistakenly executed during the configuration recovery process. On the device, the **using tengige** command takes effect in real time, but the configuration file incorrectly contains the command.

201903290556

- Symptom: Interface flapping causes the CPU usage to reach 100%.
- Condition: This symptom occurs if the following operations are performed:
  a. Multiple routes of BGP neighbors are configured with FRR. The active and backup next hops of FRR are reverse for two routes (for example, the active and backup next hops of route A are 1 and 2, and the active and backup next hops of route B are 2 and 1), and the next hops 1 and 2 are in the network segments of routes A and B.
  b. Shut down the interfaces corresponding to the two next hops in sequence.

201903290558

- Symptom: When the spanning tree mode is switched to PVST, the device will be stuck for a period of time.
- Condition: This symptom occurs if a large number of VLANs and interfaces exist on the device and the spanning tree mode is switched to PVST.

201811060535

- Symptom: When an interface card is unplugged and plugged, the aggregate interface creation event on the interface card is not reported. As a result, the aggregate interface on the interface card is not set to the drive, and the aggregate interface member ports cannot forward traffic.
- Condition: This symptom occurs because the interface management module does not report the aggregate interface creation event during the startup process when an interface card is plugged.
- Occurrence probability: This symptom occurs only when interface events are not reported. In an environment, there are a large number of interface events. In a complicated environment, the occurrence probability is high. In a test environment, the occurrence probability is low.

201807060250

- Symptom: Some traffic is broadcast on a DR interface.
- Condition: This symptom occurs if an aggregate interface leaves and then joins a DR group and continuously receives traffic.

201903110087

- Symptom: The BFD session on a Layer 3 aggregate interface flaps.
- Condition: This symptom occurs if the following operations have been performed:
  a. Configure a Layer 3 aggregate interface with member ports on different cards, enable BFD for OSPF, and use MD5 authentication for BFD control packets.
  b. Remove a member port from the Layer 3 aggregation group and then add it back to the aggregation group.

201806040598

- Symptom: The secure MAC address entry is not removed from the **display mac-address** command after a user goes offline.
- Condition: This symptom occurs if port security is configured and the user goes offline after passing authentication.

201701100257

- Symptom: Traffic detection fails in a Fabric Director scenario.
- Condition: This symptom occurs if a QoS policy is issued multiple times.

201806070741

- Symptom: The **remark dscp** command issued by OpenFlow does not take effect.
- Condition: This symptom occurs if the Output action is issued by OpenFlow at the same time.

201904020301

- Symptom: The relevant MAC address entry is not removed from the **display mac-address** command after an 802.1X user moves to a different VLAN on the same port.
- Condition: This symptom occurs if an 802.1X user moves to a different VLAN on the same port.

201904110239

- Symptom: A DR system fails to be established.
- Condition: This symptom occurs if a manually created tunnel interface is used as the IPL.

201903150058

- Symptom: In a DRNI network, the DR interface of the secondary DR device is still up after the IPP interface is brought down.
- Condition: This symptom occurs if the secondary DR device is in DRNI MAD DOWN state.

201812060999

- Symptom: In a DRNI network, the DR interface is set to DRNI DOWN state.
- Condition: This symptom might occur if the IPP interface flaps.

201805040745

- Symptom: In a multiple VSC environment, the device cannot connect to the primary VSC.
- Condition: This symptom might occur if the OVSDB process is restarted.

201810300310

- Symptom: The management Ethernet port goes down in an IRF fabric.
- Condition: This symptom might occur after a master/subordinate switchover is performed.

201711070993

- Symptom: In a VXLAN network, VMs in different network segments cannot communicate.
- Condition: This symptom occurs if a VXLAN gateway group is used as the gateway.

201805020138/201805020139

- Symptom: An additional coldStart log is printed every time the switch sends a trap.
- Condition: This symptom occurs after the switch reboots.

201904020313

- Symptom: A user can join and leave the multicast group without passing authentication.
- Condition: This symptom occurs if both MLD and IPv6 portal authentication are configured on the VLAN interface.

201903180860

- Symptom: A serial port hangs in a DRNI network.
- Condition: This symptom might occur if the following operations have been performed:
  a. Enable and disable configuration consistency check repeatedly.
  b. Execute the **display drni consistency type2 global** command.

201810100474

- Symptom: ICMPv6 packets are counted into the **IP-other** protocol type.
- Condition: This symptom occurs when the switch receives ICMPv6 packets.

201811090192

- Symptom: The MAC address entry is not removed from the **display mac-address** command after a MAC authentication user goes offline.
- Condition: This symptom occurs if the MAC authentication user comes online and then goes offline.

201904030323

- Symptom: The remote host has the TCP timestamps vulnerability.
- Condition: This symptom occurs if the host implements RFC 1323.

201812061014

- Symptom：HPE Comware 7 stored and reflected XSS Vulnerability
- Condition：An xss reflected in the web portal of the appliance HP Comware switch 7.1.045. Attackers can exploit this issue to open a web browser and log in to the application using valid or not credentials.

201812050851

- Symptom: Files in the flash might fail to be deleted at a low probability.
- Condition: This symptom occurs if multiple consoles operate the device simultaneously.

201903140269/201904020861

- Symptom: After the operating mode of a device is switched from L3GW to L2GW, the L3VNI configuration remains.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the device to operate in L3GW mode, and configure L3VNIs.
  b. Configure the device to operate in L2GW mode, save the configuration, and reboot the device.

201812280633

- Symptom: The startup configuration file on an IRF subordinate device is lost after a user logs out of the IRF fabric while the IRF fabric is saving the running configuration to the startup configuration file for the user.
- Conditions: This symptom occurs if the user logs out of the IRF fabric while the IRF fabric is saving the running configuration to the startup configuration file for the user.

Resolved problems in R2612P05

201902220726/201810240573

- Symptom: After the switch restarts up with the factory defaults, the DHCP server assigns the switch a new IP address instead of the one before the restart.
- Condition: This symptom occurs if the switch restarts up with the factory defaults and acts as a DHCP client.

201902220813

- Symptom: If VRRP groups with the same ID are configured on different VLAN interfaces, only one of the VRRP groups takes effect.
- Condition: This symptom might occur if VRRP groups with the same ID are configured on different VLAN interfaces.

201902220757

- Symptom: SNMP fails to get the MAC address of an aggregate interface from the dot1dTpFdbAddress node.
- Condition: This symptom might occur if SNMP reads the dot1dTpFdbAddress node.

201902220753/201810110532

- Symptom: After the aggregate interface of an aggregation group is assigned to an isolation group and then is removed from it, traffic received on a member port of the aggregation group is forwarded out of other member ports erroneously.
- Condition: This symptom might occur if an aggregate interface is assigned to an isolation group and then is removed from it.

201902220749

- Symptom: After queue scheduling is configured on an interface, transient traffic loss occurs on a non-related interface.
- Condition: This symptom might occur if queue scheduling is configured on an interface.

201902220748

- Symptom: The switch might generate dead loop logs when deleting multicast entries.
- Condition: This symptom might occur if the following conditions exist:
  - **a.** A large number of aggregate interfaces are configured, and they receive dense multicast traffic.
  - **b.** Aggregate interfaces are shut down.

201902220732

- Symptom: BGP sessions are interrupted.
- Condition: This symptom occurs if the following operations are performed:
  - **a.** A Layer 3 virtual interface is bound to a VPN, and a BGP neighbor relationship is established.
  - **b.** PBR is applied to the Layer 3 virtual interface.

201902220722

- Symptom: In a VCF fabric, IP addresses are re-assigned to Loopback 0 interfaces after leaf nodes automatically form an IRF fabric.
- Condition: This symptom might occur if the switch as a leaf node joins the IRF fabric automatically formed by other leaf nodes.

201902220710/201812030086

- Symptom: Packet loss might occur.
- Condition: This symptom occurs if link-aggregation traffic redirection is configured and some slots are rebooted.

201902220704/201812050851

- Symptom: Files in the flash might fail to be deleted at a low probability.
- Condition: This symptom occurs if multiple consoles operate the device simultaneously.

201902220665/201803280447

- Symptom: On an IRF fabric, the state of a VXLAN tunnel is inconsistent on the IRF master and subordinate, which causes VXLAN forwarding failure.
- Condition: This symptom might occur if VXLAN tunnels are configured on an IRF fabric.

201903131055/201903131049/201903131051

- Symptom: The PBR function might not take effect on interfaces.
- Condition: This symptom occurs if the following operations are performed:
  a. PBR is configured on multiple interfaces.
  b. Route flapping frequently occurs.

201903140301/201903140302/201709130770

- Symptom: Traffic might fail to be forwarded between VXLANs.
- Condition: This symptom occurs if the following operations are performed:
  a. The VCFC controller deploys configurations to spine and leaf devices.
  b. On a leaf device, multiple VXLANs are configured, and a large number of VMs come online.
  c. A large number of VMs migrate to other VXLANs.

Resolved problems in R2612P03

201809120302

- Symptom: Multiple copies of packets mirrored by Layer 2 remote port mirroring are received.
- Condition: This symptom occurs if the following operations are performed:
  a. Create multiple mirroring groups, and assign ports to mirroring groups.
  b. Configure reflector ports for remote mirroring groups.

201809050319/201808230872

- Symptom: After NETCONF is used to deploy the BFD-related configuration, the BFD process fails to start.
- Condition: This symptom occurs if NETCONF is used to deploy the BFD configuration.

201809050305

- Symptom: When an IPL fails, the corresponding Layer 3 interfaces cannot properly learn ARP entries. As a result, traffic is interrupted.
- Condition: This symptom occurs if the following operations are performed:
  a. In a DRNI network, configure the same MAC address for the VLAN interfaces of the VLANs to which the DR interfaces of the IPL belong.
  b. Shut down the IPL.

201809040359/201809030027/201809030023

- Symptom: After an IRF master/subordinate switchover, the AC configuration on the device might be deleted and the VM traffic cannot be forwarded at a low probability.
- Condition: This symptom occurs if the following operations are performed:
  a. On an IRF fabric, the controller automatically deploys the VXLAN function.
  b. Reboot the master IRF member device.

Resolved problems in R2612P01

201807270157/201806210622

- Symptom: When you use Director to replace the master spine device, the leaf device configuration changes.

- Condition: This symptom occurs if the automated VCF fabric deployment function is used to enable the device to cooperate with Director and implement automated configurations.

201807270712/201807270721/201807270711

- Symptom: After a master/subordinate switchover, an IRF fabric sends redundant RSCN packets to servers.
- Condition: This symptom occurs if the following operations are performed:
  a. In an FCoE network, enable hardware zoning and configure RSCN on an IRF fabric.
  b. Reboot the master IRF member device.

201808060501/201808060502/201808060503

- Symptom: The controller might fail to deploy flow entries to the subordinate IRF member devices.
- Condition: This symptom occurs if the following operations are performed:
  a. An IRF fabric acts as an OpenFlow switch and establishes a secure channel with the controller.
  b. The controller deploys flow entries to the subordinate IRF member devices.

201807270142/201806200386/201805300594

- Symptom: After the DR interface comes up, it will go down and then come up once.
- Condition: This symptom occurs if you view the DR interface status after the IPL comes up.

201807270145/201806250510/201803190222

- Symptom: A client cannot join a multicast group.
- Condition: This symptom occurs if the client comes online through portal and requests to join the multicast group in a multicast network.

201807270161/201806120577/201806270423/201806120577

- Symptom: After the reload delay timer set for a DR device expires, the DR device role is still None.
- Condition: This symptom occurs if the following operations are performed:
  a. Execute the **drni auto-recovery reload-delay** *delay-value* command to enable DR system auto-recovery and set the reload delay timer.
  b. Configure both the IPP and keepalive link to be down.
  c. Save the configuration and reboot the DR device.

201807270168/201806270402/201806070375/201806070389

- Symptom: When the **display drni role** command is used to display DR role information on the secondary DR device, the **Effective role** field displays **Primary**.
- Condition: This symptom occurs if the IPP is repeatedly shut down and brought up in a DRNI network.

201807270130/201807030034/201806290366/201806290360

- Symptom: After the whole IRF fabric is rebooted, SNMP obtains an incorrect value for the snmpEngineBoots node.
- Condition: This symptom might occur if the master member device of the IRF fabric changes after the IRF fabric is rebooted.

201807270124/201806270357/201806040701

- Symptom: The chip time is different on the master IRF member device and subordinate IRF member device.

- Condition: This symptom occurs if an IRF fabric is configured with PTP and the chip time on the master IRF member device and subordinate IRF member device is viewed.

201806260327/201807270176/201807060219

- Symptom: A DR system fails after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure a tunnel interface as the IPP.
  b. Configure dynamic tunnels on the DR member devices, and the dynamic tunnels share the destination IP address with the tunnel that acts as the IPL.
  c. Delete the IPP tunnel interface and reconfigure it.

201807270182/201807030632/201807310533

- Symptom: On the secondary DR member device, a DR interface in DRNI DOWN state is removed from its DR group. After the DR interface is reassigned to the DR group, its state becomes DOWN.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure a Layer 2 aggregate interface as a DR interface and assign it to a DR group on the secondary DR member device.
  b. Remove the DR interface from its DR group and then reassign it to the DR group when the IPL is down.

201807270188/201806010178/201807030865

- Symptom: On a DR member device, member ports of a DR interface cannot become Selected after the device is rebooted.
- Condition: This symptom might occur if the following operations are performed:
  a. Execute the **lacp edge-port** command on the DR interface.
  b. Save the configuration and reboot the DR member device.

201807270193/201807070082/201807070098

- Symptom: RSVP has memory leaks if RSVP authentication fails.
- Condition: This symptom might occur if RSVP authentication fails.

201807270196/201807100205/201807100209

- Symptom: Memory leaks occur if the switch repeatedly generates and deletes a large number of multicast entries.
- Condition: This symptom might occur if the switch repeatedly generates and deletes a large number of multicast entries.

201807060212/201807270199/201807060355

- Symptom: DR member devices might fail to forward Layer 3 traffic after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure a VXLAN tunnel interface as the IPP of the DR system.
  b. Configure the DR member devices to establish dynamic tunnels to external networks.
  c. Delete the VXLAN tunnel interface.
  d. Shut down and then bring up the interfaces connected to the external networks.
  e. Create a VXLAN tunnel interface and configure it as the IPP.

201807270206/201806290774/201807100295

- Symptom: Third-party services, service chain, and PBR are configured on an 5940 switch that acts as a leaf node in a VCF fabric. After the **reset arp all** command is executed, PBR configuration does not take effect.
- Condition: This symptom might occur if the **reset arp all** command is executed on the 5940 switch.

201807270207/201806280646/201806270600

- Symptom: Memory leaks for the OVSDB module. About 50 bytes leak every 10 seconds. If the controller re-deploys the configuration, about 80 bytes leak.
- Condition: This symptom occurs if the device has the OVSDB service enabled, and the data in the OVSDB database are modified after the controller deploys a global table containing the master controller IP to the OVSDB database.

201807170279/201807270285/201804100876

- Symptom: The device name configured for a device by using the **sysname** command does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure automated underlay network deployment on the device.
  b. Use the **sysname** command to modify the device name, save the configuration, and reboot the device.

201807270468/201805220131

- Symptom: After the device runs for a period of time, the MACsec data packets cannot be forwarded.
- Condition: This symptom occurs if the device acts as a MACsec client and establishes a device-oriented MACsec network with a Huawei or Cisco device.

201807270215/201806260106/201806250611

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if an aggregation group has more than 32 member ports and any member port leaves the aggregation group.

201808210067

- Symptom: If the **undo irf mac-address persistent** command is executed on an IRF fabric configured with VXLAN, overlay traffic forwarding fails after an IRF master/subordinate switchover.
- Condition: This symptom might occur if the **undo irf mac-address persistent** command is executed on an IRF fabric configured with VXLAN, and an IRF master/subordinate switchover occurs.

Resolved problems in R2612

201805120143/201805120129

- Symptom: Auto-RP listening does not take effect.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable Auto-RP listening on the device.
  b. Configure a Layer 2 aggregate interface as a trunk port and assign it to a VLAN.
  c. Enable PIM-SM on the VLAN interface.

201805110585

- Symptom: On a DRNI+STP network, traffic interruption occurs after the IPL goes down and then comes up.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure an aggregate interface on each DR member device as the IPP.
  b. Reboot a DR member device so that the DR member devices are assigned new roles.

201805110581/201803270029

- Symptom: On a DRNI+STP network where the DR system operates correctly, it takes DR interfaces ten minutes to come up after they are set to DRNI MAD DOWN state.
- Condition: This symptom might occur if a DR member device reboots and then the IPP goes down.

201805110456

- Symptom: The ovsdb-server process exits unexpectedly.
- Condition: This symptom might occur after a VTEP is enabled with the OVSDB server feature and establishes an OVSDB connection with the controller.

201805090685

- Symptom: An IRF subordinate device reboots unexpectedly after the **display interface** command is executed on the IRF fabric.
- Condition: This symptom might occur if Layer 3 Ethernet subinterfaces are created on the IRF fabric.

201805070301

- Symptom: The OVSDB connection to the controller is disconnected after a length of time since a VTEP has been enabled with the OVSDB server feature and established an OVSDB connection to the controller.
- Condition: This symptom might occur after a length of time since a VTEP has been enabled with the OVSDB server feature and established an OVSDB connection to the controller.

201805050184

- Symptom: The device fails to set the VXLAN hardware resource mode.
- Condition: This symptom might occur if the following operations:
  a. Set the VXLAN hardware resource mode.
  b. Save the running configuration and reboot the device.
  c. Use the **display hardware-resource** command to display the VXLAN hardware resource mode. The displayed hardware resource mode is not the specified one.

201805100244

- Symptom: The remote fault signal detection feature, which is supported only on fiber ports, can be enabled on copper ports.
- Condition: This symptom might occur if the **link-fault-signal enable** command is executed on copper ports.

201805090323

- Symptom: The system prompts unsupported operation if the speed of a 100-GE interface is repeatedly changed between 100000 Mbps and 10000 Mbps.
- Condition: This symptom might occur if the speed of a 100-GE interface is repeatedly changed between 100000 Mbps and 10000 Mbps by using the **speed 100000** and **speed 10000** commands.

201805040458

- Symptom: The memory of the QACL module slowly leaks.
- Condition: This symptom occurs if actions in traffic behaviors are dynamically modified repeatedly.

201805020139

- Symptom: The device prints coldStart traps unexpectedly when printing port security traps.
- Condition: This symptom occurs when the device is rebooted and prints port security traps.

201805020133

- Symptom: When the device learns secure MAC address entries, it prints the same traps for twice.
- Condition: This symptom occurs if the device has port security enabled and is configured with secure MAC address entries.

201804250026

- Symptom: The Connect Retry timer times out. As a result, BGP might flap.
- Condition: This symptom occurs if the following operations are performed:
  a. On an IRF fabric, configure BGP NSR.
  b. Reboot the device after the device has run for a long period of time.

201803270632

- Symptom: The 802.1p-to-local priority map might be modified.
- Condition: This symptom occurs if the following operations are performed:
  a. Split a 100-GE interface into four breakout interfaces.
  b. Configure the 802.1p-to-local priority map.
  c. Combine the breakout interfaces into a 100-GE interface.

201804170805

- Symptom: An interface fails to join an aggregation group.
- Condition: This symptom occurs if the following operations are performed:
  a. Execute the **vtep access port** command to specify a site-facing interface as a VTEP access port.
  b. Create an aggregation group, and assign the interface to the aggregation group.

201804160611

- Symptom: When the TTL in IPv6 BGP protocol packets is 1, the packets mistakenly match an ACL used for matching IPv6 packets with TTL as 1. As a result, the link flaps.
- Condition: This symptom occurs if IPv6 BGP protocol packets with TTL as 1 are received.

201804120615

- Symptom: A user cannot log in to the device by using NETCONF after certain operations when password control is enabled.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable password control on the device.
  b. Repeatedly establish and delete sessions, and perform active/standby process switchover.
  c. Log in to the device by using NETCONF.

201804120137

- Symptom: In a DRNI network, MAC address entries fail to be synchronized between the primary and secondary devices.
- Condition: This symptom occurs if the following operations are performed:
  a. In a DRNI, execute the **shutdown** and **undo shutdown** commands on the IPP.
  b. The device receives a large number of Layer 2 packets with changing source MAC addresses.

201803150880

- Symptom: VLAN-based VXLAN assignment configuration cannot be restored by using an .mdb binary file.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure a large number of VSIs and enable VLAN-based VXLAN assignment.
  b. Save the configuration, reboot the switch, and use an .mdb binary file to restore the configuration.

201802280277

- Symptom: The controller cannot discover the site-facing interfaces configured by using **vtep access port** if the switch uses Chinese GB2312 characters as the sysname.
- Condition: This symptom might occur if the sysname of the switch contains Chinese GB2312 characters.

201805150032/201712060462/201712060449

- Symptom: The switch reboots unexpectedly.
- Condition: This symptom occurs if the debugging command is used to disable the linkscan for interfaces.

201805100905/201805100908

- Symptom: The switch acts as a VXLAN VTEP, and an Ethernet service instance that uses the **encapsulation default** criterion is configured on an aggregate interface. After the aggregate interface is shut down and then brought up, traffic received on the Ethernet service instance cannot be forwarded correctly.
- Condition: This symptom might occur if an Ethernet service instance that uses the **encapsulation default** criterion is configured on an aggregate interface, and the aggregate interface is shut down and then brought up.

201804240046/201802240168/201709010504

- Symptom: ACLs might remain at a low probability after certain operations.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure a routing policy, and specify the next hop of the routing policy as a GRE tunnel interface.
  b. Modify the source IP address of the GRE tunnel.

201805290161/201805280462

- Symptom: Disabling MAC address learning does not take effect on a Layer 2 aggregate interface.
- Condition: This symptom occurs if the following operations are performed:
  a. Disable MAC address learning globally.
  b. In the view of a Layer 2 aggregate interface, execute the **undo mac-address mac-learning enable** command to disable MAC address learning.

201805290049/201805280775

- Symptom: The CLI does not respond after password control is disabled.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable Password Control on the device. A large number of invalid NETCONF users log in to the device.
  b. Disable password control.

201805250503/201805250377

- Symptom: Some ACL resources remain.
- Condition: This symptom occurs if the following operations are performed:
  a. The switch operates in FCF mode and connects to multiple nodes.
  b. Modify the bridge MAC address of the switch.

201805240699/201805220499

- Symptom: The device prints deadloop logs when the **step** command is used to modify the rule numbering step for an ACL.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure a PBR policy on the device, and configure rules for the ACL that the PBR policy uses.
  b. Apply the PBR policy to packets that an interface forwards.
  c. Enter the view of the ACL, and use the **step** command to set the rule numbering step.

201805240599/201805150488

- Symptom: OpenFlow is disconnected from the controller.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure OpenFlow on the device and establish a connection to the controller.
  b. The interface corresponding to the AC is frequently shut down and brought up.

201805310080/201805310084/201805310093

- Symptom: The broadcast packets received on a member port of an aggregation group might be broadcast out of other member ports of the aggregation group.
- Condition: This symptom occurs if the following operations are performed:
  a. Assign local ports to an aggregation group. Delete the aggregation group. Restore the default settings for member ports, and then assign these ports to the aggregation group.
  b. Execute the **shutdown** and **undo shutdown** command sequence on the aggregation group member ports.
  c. Switch the mode of the aggregation group to dynamic or static.
  d. The local device is an STP root bridge. An interface on the peer device repeatedly flaps, and the peer device sends TCN BPDUs.

Resolved problems in R2611

First release.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect:

- Technical support registration number (if applicable).
- Product name, model or version, and serial number.
- Operating system name and version.
- Firmware version.
- Error messages.
- Product-specific reports and logs.
- Add-on products or components.
- Third-party products or components.

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website at http://www.hpe.com/support/hpesc.

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see HPE FlexNetwork technology acronyms.

Related documents

The following documents provide related information:

- *HPE PSR250-A & PSR250-A1 Power Supplies User Guide*
- *HPE FlexFabric X721 Front-to-Back (JL594) & X722 Back-to-Front (JL595) Fan Trays User Guide*
- *HPE PSR450 Power Supply Series User Guide*
- *HPE FlexFabric 5710 Switch Series Installation Guide*
- *HPE FlexFabric 5710 Switch Series Configuration Guides*-Release 671x
- *HPE FlexFabric 5710 Switch Series Command References*-Release 671x

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Appendix A Fixed security vulnerabilities

Fixed security vulnerabilities in R6710

CVE-2020-7469

In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 the handler for a routing option caches a pointer into the packet buffer holding the ICMPv6 message. However, when processing subsequent options the packet buffer may be freed, rendering the cached pointer invalid. The network stack may later dereference the pointer, potentially triggering a use-after-free.

CVE-2021-22924

*libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse, if one of them matches the setup.Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections.File paths are, or can be, case sensitive on many systems but not all, and caneven vary depending on used file systems.The comparison also didn't include the 'issuer cert' which a transfer can setto qualify how to verify the server certificate.*

CVE-2022-0778

The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

CVE-2013-2566

The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

CVE-2015-2808

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing

network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

CVE-2015-0204

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations

Fixed security vulnerabilities in R2702

CVE-2018-5407

OpenSSL is prone to a local information-disclosure vulnerability. Local attackers can exploit this issue to obtain sensitive information. This may aid in further attacks.

CVE-2018-15473

OpenSSH is prone to a user-enumeration vulnerability. An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks. OpenSSH through 7.7 are vulnerable; other versions may also be affected.

Fixed security vulnerabilities in R2612

CVE-2017-12190

Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

CVE-2017-12192

Attackers can exploit this issue to cause denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

CVE-2017-15274

An attacker can exploit this issue to cause a local denial-of-service condition.

CVE-2017-15299

An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.

Appendix B Feature list

Hardware features

Table 5 5710 48SFP+ 6QS+/2QS28 Switch and 24SFP+ 6QS+/2QS28 Switch hardware features

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 24SFP+ 6QS+/2QS28 Switch JL587A
Dimensions (H × W × D)	44 × 440 × 400 mm (1.73 × 17.32 × 15.75 in)	44 × 440 × 400 mm (1.73 × 17.32 × 15.75 in)
Weight	≤ 10 kg (22.05 lb)	≤ 10 kg (22.05 lb)

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 24SFP+ 6QS+/2QS28 Switch JL587A
Console ports	• 1 × mini USB console port • 1 × serial console port	• 1 × mini USB console port • 1 × serial console port
Management Ethernet ports	• 1 × 10M/100M/1000MBASE-T copper port • 1 × SFP port	• 1 × 10M/100M/1000MBASE-T copper port • 1 × SFP port
USB ports	1	1
1/10GBASE-T autosensing Ethernet ports	N/A	N/A
SFP+ ports	48	24
QSFP+ ports	Up to 6	Up to 6
QSFP28 ports	Up to 2	Up to 2
Fan tray slots	4	4
Power supply slots	2	2
Input voltage	PSR250-12A/PSR250-12A1/PSR450-12A/PSR450-12A1: • Rated voltage: 100 to 240 VAC @ 50/60 Hz • Max voltage: 90 to 290 VAC @ 47 to 63 Hz PSR450-12D: • Rated voltage: –48 to –60 VDC • Max voltage: –36 to –72 VDC	
Minimum power consumption	PSR250-12A/PSR250-12A1: • Single AC input: 66 W • Dual AC inputs: 74 W PSR450-12A/PSR450-12A1: • Single AC input: 68 W • Dual AC inputs: 76 W PSR450-12D: • Single DC input: 68 W • Dual DC inputs: 73 W	PSR250-12A/PSR250-12A1: • Single AC input: 66 W • Dual AC inputs: 74 W PSR450-12A/PSR450-12A1: • Single AC input: 67 W • Dual AC inputs: 76 W PSR450-12D: • Single DC input: 68 W • Dual DC inputs: 74 W
Maximum power consumption	PSR250-12A/PSR250-12A1: • Single AC input: 171 W • Dual AC inputs: 178 W PSR450-12A/PSR450-12A1: • Single AC input: 169 W • Dual AC inputs: 178 W PSR450-12D: • Single DC input: 169 W • Dual DC inputs: 176 W	PSR250-12A/PSR250-12A1: • Single AC input: 130 W • Dual AC inputs: 134 W PSR450-12A/PSR450-12A1: • Single AC input: 130 W • Dual AC inputs: 138 W PSR450-12D: • Single DC input: 133 W • Dual DC inputs: 140 W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power supply	PSR250-12A/PSR250-12A1: 6.3 A @ 250 VAC PSR450-12A/PSR450-12A1: 10 A @ 250 VAC	

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 24SFP+ 6QS+/2QS28 Switch JL587A
fuse	PSR450-12D: 20 A @ 125 VDC	
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	10% RH to 90% RH, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

Table 6 5710 48XGT 6QS+/2QS28 Switch and 24XGT 6QS+/2QS28 Switch hardware features

Item	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24XGT 6QS+/2QS28 Switch JL689A
Dimensions (H × W × D)	44 × 440 × 460 mm (1.73 × 17.32 × 18.11 in)	44 × 440 × 460 mm (1.73 × 17.32 × 18.11 in)
Weight	≤ 10 kg (22.05 lb)	≤ 10 kg (22.05 lb)
Console ports	• 1 × mini USB console port • 1 × serial console port	• 1 × mini USB console port • 1 × serial console port
Management Ethernet ports	• 1 × 10M/100M/1000MBASE-T copper port • 1 × SFP port	• 1 × 10M/100M/1000MBASE-T copper port • 1 × SFP port
USB ports	1	1
1/10GBASE-T autosensing Ethernet ports	48	24
QSFP+ ports	Up to 6	Up to 6
QSFP28 ports	Up to 2	Up to 2
Fan tray slots	5	4
Power supply slots	2	2
Input voltage	-	PSR250-12A/PSR250-12A1/PSR450-12A/PSR450-12A1: • Rated voltage: 100 to 240 VAC @ 50/60 Hz • Max voltage: 90 to 290 VAC @ 47 to 63 Hz
	PSR450-12A/PSR450-12A1: • Rated voltage: 100 to 240 VAC @ 50/60 Hz • Max voltage: 90 to 290 VAC @ 47 to 63 Hz PSR450-12D: • Rated voltage: –48 to –60 VDC • Max voltage: –36 to –72 VDC	
Minimum power consumption	PSR450-12A/PSR450-12A1: • Single AC input: 101 W • Dual AC inputs: 108 W PSR450-12D: • Single DC input: 97 W • Dual DC inputs: 104 W	PSR250-12A/PSR250-12A1: • Single AC input: 77 W • Dual AC inputs: 83 W PSR450-12A/PSR450-12A1: • Single AC input: 78 W • Dual AC inputs: 87 W

Item	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24XGT 6QS+/2QS28 Switch JL689A
		PSR450-12D: • Single DC input: 78 W • Dual DC inputs: 85 W
Maximum power consumption	PSR450-12A/PSR450-12A1: • Single AC input: 255 W • Dual AC inputs: 258 W PSR450-12D: • Single DC input: 259 W • Dual DC inputs: 264 W	PSR250-12A/PSR250-12A1: • Single AC input: 177 W • Dual AC inputs: 183 W PSR450-12A/PSR450-12A1: • Single AC input: 176 W • Dual AC inputs: 182 W PSR450-12D: • Single DC input: 175 W • Dual DC inputs: 182 W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power supply fuse	-	PSR250-12A/PSR250-12A1: 6.3 A @ 250 VAC
	PSR450-12A/PSR450-12A1: 10 A @ 250 VAC PSR450-12D: 20 A @ 125 V	
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	10% RH to 90% RH, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

Software features

Table 7 Software features of the 5710 series

Item		5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
Line-rate Layer 2 switching	Switching capacity (full duplex)	1440 Gbps	1440G bps	960 Gbps	
	Packet forwarding capacity(chassis)	1071.36	1071.36	714.24	
Forwarding mode		Store-forward			
IRF		• IRF fabric in daisy-chain topology • IRF fabric in ring topology • LACP MAD • ARP MAD • ND MAD • BFD MAD • ISSU			

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
	• Heterogeneity of IRF members			
Link aggregation	• 10GE/40GE/100GE port aggregation • Static aggregation • Dynamic aggregation • A maximum of 1K aggregation groups and a maximum of 32 selected ports per group in an IRF fabric • NLB • DNRI			
Data center	• PFC, VXLAN PFC • QCN • ETS • DCBX • OpenFlow • VXLAN • VXLAN L3 Gateway			
Flow control	• 802.3x flow control • Back pressure			
Jumbo frame	A maximum of 10000 bytes			
MAC address table	• A maximum of 208K MAC address entries • A maximum of 1K static MAC address entries • Blackhole MAC address entries • MAC learning limit on interfaces			
VLAN	• Port-based VLAN (quantity: 4094) • QinQ and flexbile QinQ • Voice VLAN • Protocol-based VLAN • MAC-based VLAN • IP subnet-based VLAN • Super VLAN			
VLAN mapping	• 1:1 • N:1 • 2:2			
ARP	• A maximum of 68K ARP entries • A maximum of 1K static ARP entries • Gratuitous ARP • Common proxy ARP and local proxy ARP • ARP source-suppression • ARP blackhole • ARP attack detection based on DHCP snooping entries, 802.1X entries, or IP/MAC static binding entries • Multicast ARP			
ND	• A maximum of 34K ND entries • A maximum of 1K static ND entries • RA guard • ND snooping • ND detection			

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
VLAN virtual interfaces	1K			
DHCP	• DHCP client • DHCP snooping • DHCP relay • DHCP server • DHCPv6 server			
UDP helper	Supported			
DNS	• Static domain name resolution • Dynamic domain name resolution • IPv4 and IPv6 addresses			
IPv4 routing	• A maximum of 4K static routes • RIPv1/v2, a maximum of 4K IPv4 routes • OSPFv1/v2, a maximum of 16K IPv4 routes • BGP, a maximum of 16K IPv4 routes • ISIS, a maximum of 16K IPv4 routes • 511 ECMP groups, a maximum of 128 routes per group; a maximum of 16K ECMP routes per chassis • Routing policy • VRRP • Policy-based routing			
IPv6 routing	• A maximum of 2K static routes • RIPng, a maximum of 2K IPv6 routes • OSPFv3, a maximum of 8K IPv6 routes • BGP4+ for IPv6, a maximum of 8K IPv6 routes • ISISv6, a maximum of 8K IPv6 routes • 511 ECMP groups, a maximum of 128 routes per group, a maximum of 16K ECMP routes per chassis • Routing policy • VRRP • Policy-based routing			
URPF	Supported			
MCE	Supported			
BFD	• OSPF/OSPFv3 • BGP/BGP4 • IS-IS/IS-IS IPv6 • PIM IPv6 • Static Route • MAD			
Tunnel	• IPv4 over IPv4 tunnel • IPv4 over IPv6 tunnel • IPv6 over IPv4 manual tunnel • IPv6 over IPv4 6to4 tunnel • IPv6 over IPv4 Intra-site Automatic Tunneling Protocol (ISATAP) tunnel • IPv6 over IPv6 tunnel • GRE tunnel			

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
IPv4 multicast	• Internet Group Management Protocol (IGMP) Snooping v1/v2/v3 • Multicast VLAN • IGMPv1/v2/v3 • Protocol Independent Multicast-Dense Mode (PIM-DM) • Protocol Independent Multicast-Sparse Mode (PIM-SM) • PIM-SSM • Multicast Source Discovery Protocol (MSDP) • BIDIR-PIM • Multicast MCE • Multicast VPN • Multicast tunnel			
IPv6 multicast	• MLD Snooping v1/v2 • MLDv1/v2 • PIM-DM/SM/SSM for IPv6 • PIM-SSM for IPv6 • IPv6 BIDIR-PIM • IPv6 PIM snooping • IPv6 multicast VLAN			
Broadcast/multicast/unicast storm suppression	• Storm suppression based on port bandwidth percentage • Storm suppression based on PPS/BPS			
MSTP	• STP/RSTP/MSTP • STP root guard • BPDU guard			
PVST+	510 PVST+ instances			
RRPP	• RRPP protocol • RRPP multiple instances			
Smart Link	• 48 mart link groups • Smart Link multiple instances			
Monitor Link	Supported			
QoS/ACL	• Port-based rate limit (a minimum CIR of 8 Kbps) • Traffic redirection • Committed access rate (CAR) with a minimum granularity of 8 kbps • 8 output queues per port • Flexible queuing and scheduling algorithms configured on a per-port or per-queue basis, including strict priority (SP), weighted round robin (WRR), SP+WRR, weighted fair queuing (WFQ), and SP+WFQ • Queue scheduling profile • 802.1p and DSCP priority marking • Packet filtering based on packet header fields from Layer 2 through Layer 4, including source MAC, destination MAC, source IP (IPv4/IPv6), destination IP (IPv4/IPv6), port number, protocol type, and VLAN • Time range • Weighted Random Early Detection (WERD) • Queue shaping • COPP			

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
	• Aggregate CAR • ECN			
Mirroring	• Flow mirroring • Port mirroring • Multiple monitor ports			
Remoting mirroring	RSPAN/ERSPAN			
Security	• Hierarchical user management and password protection • AAA • RADIUS • HWTACACS • SSH 2.0 • Port isolation • Port security • MAC address authentication • IP address, MAC address, and port number binding • IP source guard • HTTPS • SSL • Public Key Infrastructure (PKI) • Portal			
802.1X	• A maximum of 2048 users • Port-based access control and MAC-based access control • Guest VLAN • Trunk port authentication • Dynamic assignment of QoS/ACL/VLAN based on 802.1X • VSI manipulation			
Flow management	sFlow			
Loading and upgrading	• Loading/upgrading through the XMODEM protocol • Loading/upgrading through FTP and TFTP			
Management	• Configuration at the CLI • Telnet configuration • Configuration through the console port • Simple Network Management Protocol (SNMP) • Remote Network Monitoring (RMON) • IMC • NETCONF • System logs • Hierarchical alarms • NTP • Power supply status alarming • Fan tray status alarming • Temperature alarming			
Maintenance	• Debugging information output • Ping and tracert • NQA • Track			

Item	5710 48SFP+ 6QS+/2QS28 Switch JL585A	5710 48XGT 6QS+/2QS28 Switch JL586A	5710 24SFP+ 6QS+/2QS28 Switch JL587A	5710 24XGT 6QS+/2QS28 Switch JL689A
	• Telnet • 802.1ag • 802.3ah • DLDP			

Appendix C Upgrading software

This section describes how to upgrade system software while the router is operating normally or when the router cannot correctly start up.

System software file types

Software required for starting up the switch includes:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the switch cannot correctly start up.
- **Software images**—Includes boot images and system images.
  - **Boot image**—A .bin file that contains the operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
  - **System** image—A .bin file that contains the main application code required for device operation. This includes device management, interface management, configuration management, and routing management.

The software images that have been loaded are called "current software images." The software images specified to load at next startup are called "startup software images."

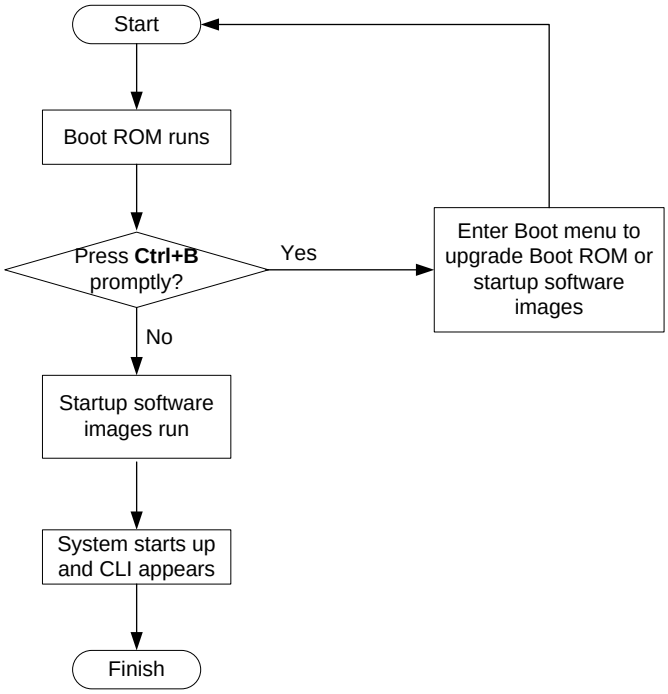
These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images in the file and sets them as startup software images. Typically, the Boot ROM and software images for this switch series are released in an .ipe file named **main.ipe**.

In addition to these images, HPE irregularly releases patch packages for you to fix bugs without rebooting the switch. A patch package does not add new features or functions.

System startup process

Upon power-on, the Boot ROM image runs to initialize hardware and then the software images run to start up the entire system, as shown in Figure 1.

Figure 1 System startup process



Upgrade methods

You can upgrade system software by using one of the following methods:

Upgrading method	Software types	Remarks
Upgrading from the CLI	Software images	• You must reboot the switch to complete the upgrade. • This method can interrupt ongoing network services.
	Patch packages	The upgrade does not interrupt ongoing services. Make sure the patch packages match the current software images. A patch package can fix bugs only for its matching software image version.
Upgrading from the Boot menu	• Boot ROM image • Software images	Use this method when the switch cannot correctly start up. **CAUTION:** Upgrading an IRF fabric from the CLI rather than the Boot menu. The Boot menu approach requires that you upgrade the member switches one by one and has larger impact on services than the CLI approach.

The output in this document is for illustration only and might vary with software releases. For example, this document uses boot.bin and system.bin to represent boot and system image names, whereas the actual software image name format is chassis_software platform version_image type_release, for example, 5710-cmw710-boot-r2506.bin and 5710-cmw710-system-r2506.bin.

Upgrading from the CLI

This section uses a two-member IRF fabric as an example to describe how to upgrade software from the CLI. If you have more than two subordinate switches, repeat the steps for the subordinate switch to upgrade their software. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch.

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

1. Log in to the IRF fabric through Telnet or the console port (details not shown).
2. Perform the **display irf** command in any view to identify the number of IRF members, each member switch's role and IRF member ID.

```
<Sysname> display irf
MemberID   Role   Priority  CPU-Mac         Description
 *+1       Master  5         0023-8927-afdc  ---
   2       Standby 1         0023-8927-af43  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-8927-afdb
 Auto upgrade               : no
 Mac persistent             : 6 min
 Domain ID                  : 0
```

3. Perform the **dir** command in user view to identify the free storage space of each member switch.
4. Identify the free Flash space of the master switch.

```
<Sysname> dir
Directory of flash:
     0      -rw-       41424  Aug 23 2013 00:33:57     startup.mdb
     1      -rw-        3792  Aug 23 2013 00:33:56     startup.cfg
     2      -rw-    53555200  Aug 23 2013 16:04:08     system.bin
     3      drw-           -  Aug 23 2013 00:03:07     seclog
     4      drw-           -  Aug 23 2013 00:03:07     diagfile
     5      drw-           -  Aug 23 2013 00:03:07     logfile
     6      -rw-     9959424  Aug 23 2013 16:04:08     boot.bin
     7      -rw-     9012224  Aug 21 2013 09:54:27     backup.bin

1048576 KB total (977704 KB free)
```

5. Identify the free Flash space of each subordinate switch, for example, switch 2.

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:/
     0      -rw-       41424  Aug 23 2013 00:33:57     startup.mdb
     1      -rw-        3792  Aug 23 2013 00:33:56     startup.cfg
     2      -rw-    93871104  Aug 23 2013 16:00:08     system.bin
     3      drw-           -  Aug 23 2013 00:03:07     seclog
     4      drw-           -  Aug 23 2013 00:03:07     diagfile
```

```
5       drw-           -  Aug 23 2013 00:03:07     logfile
6       -rw-    13611008  Aug 23 2013 15:59:00     boot.bin
7       -rw-     9012224  Aug 21 2013 09:54:27     backup.bin

1048576 KB total (934767 KB free)
```

6. Compare the free Flash space of each member switch with the size of the software file to load. If the space is sufficient, start the upgrade process. If not, go to the next step.
7. Delete obsolete files in Flash to free space:

CAUTION:

- To avoid data loss, do not delete the current configuration file. For information about the current configuration file, perform the **display startup** command. Hewlett Packard Enterprise recommends that you preferentially delete obsolete software images. To avoid inadvertent delete of the current software images, perform the **display boot-loader** command in any view to identify them.
- The **delete /unreserved** *file-url* command deletes a file permanently and the action cannot be undone.
- The **delete** *file-url* command moves a file to the recycle bin and the file still occupies storage space. To permanently delete the file from the recycle bin, first perform the **undelete** command to restore the file and then perform the **delete /unreserved** *file-url* command.

8. Delete obsolete files from the Flash memory of the master switch.

```
<Sysname> delete /unreserved flash:/backup.bin
The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/backup.bin...Done.
```

9. Delete obsolete files from the Flash memory of the subordinate switch.

```
<Sysname> delete /unreserved slot2#flash:/backup.bin
The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file slot2#flash:/backup.bin...Done.
```

Downloading software to the master switch

Before you start upgrading software images or patch packages, make sure you have downloaded the upgrading software files to the root directory in Flash memory. This section describes downloading an .ipe software file as an example.

The following are ways to download, upload, or copy files to the master switch:

- FTP download from a server
- FTP upload from a client
- TFTP download from a server
- Copying files from a USB flash drive

Prerequisites

If FTP or TFTP is used, the IRF fabric and the PC working as the FTP/TFTP server or FTP client can reach each other.

Prepare the FTP server or TFTP server program yourself for the PC. The switch series does not come with these software programs.

FTP download from a server

You can use the switch as an FTP client to download files from an FTP server.

To download a file from an FTP server, for example, the server at 10.10.110.1:

1. Run an FTP server program on the server, configure an FTP username and password, specify the working directory and copy the file, for example, **newest.ipe**, to the directory.
2. Perform the **ftp** command in user view on the IRF fabric to access the FTP server.

```
<Sysname> ftp 10.10.110.1
Trying 10.10.110.1...
Press CTRL+K to abort
Connected to 10.10.110.1
220 FTP service ready.
User(10.10.110.1:(none)):username
331 Password required for username.
Password:
230 User logged in
```

3. Enable the binary transfer mode.

```
ftp> binary
  200 Type set to I.
```

4. Perform the **get** command in FTP client view to download the file from the FTP server.

```
ftp> get newest.ipe
  227 Entering Passive Mode (10,10,110,1,17,97).
  125 BINARY mode data connection already open, transfer starting for /newest.ipe
  226 Transfer complete.
  63521792 bytes received in 35 seconds (896. 0 kbyte/s)
ftp> bye
221 Server closing.
```

FTP upload from a client

You can use the IRF fabric as an FTP server and upload files from a client to the IRF fabric.

To FTP upload a file from a client:

1. On the IRF fabric:
2. Enable FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

3. Add a local FTP user account, set its password and access service type, and assign it to the user role network-admin for uploading file to the working directory of the server.

```
[Sysname] local-user abc
[Sysname-luser-manage-abc] password simple pwd
[Sysname-luser-manage-abc] service-type ftp
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
[Sysname-luser-manage-abc] quit
[Sysname] quit
```

4. On the PC:
5. FTP to the IRF fabric (the FTP server).

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

6. Enable the binary file transfer mode.

```
ftp> binary
200 TYPE is now 8-bit binary.
```

7. Upload the file (for example, **newest.ipe**) to the root directory in the Flash memory of the master switch.

```
ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 63521792 bytes sent in 64.58 secs (497.60 Kbytes/sec).
```

TFTP download from a server

To download a file from a TFTP server, for example, the server at 10.10.110.1:

1. Run a TFTP server program on the server, specify the working directory, and copy the file, for example, **newest.ipe**, to the directory.
2. On the IRF fabric, perform the **tftp** command in user view to download the file to the root directory in the Flash memory of the master switch.

```
<Sysname> tftp 10.10.110.1 get newest.ipe
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 60.5M    0 60.5M    0     0   143k      0 --:--:--  0:03:38 --:--:--  142k
```

Copying files from a USB flash drive

Every 5710 switch provides a USB port for you to copy files from a USB flash drive.

To copy a file from a USB flash drive to the Flash memory of the master switch:

1. Plug the USB flash drive in the USB port of the switch.
2. Copy the file (for example, **newest.ipe**) to the Flash memory of the switch.

```
<Sysname> cd usba:
<Sysname> copy usba:/newest.ipe newest.ipe
Copy usba:/newest.ipe to flash:/newest.ipe?[Y/N]:y
Start to copy usba:/newest.ipe to flash:/newest.ipe... Done.
```

Upgrading the software images

To upgrade the software images:

1. Specify the upgrading image file (**newest.ipe** in this example) used at the next startup for the master switch, and assign the M attribute to the boot and system images in the file.

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
Verifying image file....Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

2. Specify the upgrading image file used at next startup for the subordinate switch, and assign the M attribute to the boot and system images in the file. (As a result, the subordinate switch automatically copies the file to the root directory in its Flash memory.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
Verifying image file....Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
```

3. (Optional) If the IRF fabric size has a lot of members, enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
[Sysname] quit
```

Software auto-update is typically used for synchronizing the software images of the master switch to new member switches when you expand the IRF fabric. This function enables a subordinate switch to compare its main startup software image version with that of the IRF master. If the versions are different, the subordinate switch automatically downloads the current software images from the master, sets the downloaded images as the main software images at the next reboot, and automatically reboots with the new images to re-join the IRF fabric. In this upgrade process, the function avoids the failure of assign all the subordinate switch the same main software image file as the master switch causing an upgrade failure.

4. Save the current configuration in any view to prevent data loss.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.................
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
This command will reboot the device. Continue? [Y/N]:y
 Now rebooting, please wait...
```

   The system automatically loads the .bin boot and system images in the .ipe file and sets them as the startup software images.

6. Perform the **display version** command in any view to verify that the current main software images have been updated (details not shown).

NOTE:

The system automatically checks the compatibility of the Boot ROM image and the boot and system images during the reboot. If you are prompted that the Boot ROM image in the upgrading image file is different than the current Boot ROM image, upgrade both the basic and extended sections of the Boot ROM image for compatibility. If you choose to not upgrade the Boot ROM image, the system will ask for an upgrade at the next reboot performed by powering on the switch or rebooting from the CLI (promptly or as scheduled). If you fail to make any choice in the required time, the system upgrades the entire Boot ROM image.

Installing a patch package

To install a patch package, for example, **system-patch.bin**:

1. Activate the patch package on the master switch and the subordinate switch.

```
<Sysname> install activate patch flash:/system-patch.bin slot 1
<Sysname> install activate patch flash:/system-patch.bin slot 2
```

2. Verify that the patch package has been activated.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
Active packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
```

3. Commit the installation so the patch package continues to take effect after a reboot.

```
<Sysname> install commit
```

4. Verify that the patch package installation has been committed.

```
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
Committed packages on slot 2:
  flash:/boot.bin
  flash:/system.bin
  flash:/system-patch.bin
```

For more information about installing patch packages, see HPE FlexFabric 5710 Switch Series Fundamentals Configuration Guide.

Upgrading from the Boot menu

You can upgrade the Boot ROM image and software images but not patch packages from the Boot menu.

In this approach, you must access the Boot menu of each member switch to upgrade their software one by one. If you are upgrading software images for an IRF fabric, using the CLI is a better choice.

The following sections describe the methods of upgrading software images:

- Using TFTP to upgrade software images through the management Ethernet port
- Using FTP to upgrade software through the management Ethernet port
- Using XMODEM to upgrade software through the console port

The following sections describe the methods of upgrading Boot ROM images:

- Using TFTP to upgrade Boot ROM through the management Ethernet port
- Using FTP to upgrade Boot ROM through the management Ethernet port
- Using XMODEM to upgrade Boot ROM through the console port

TIP:

Upgrading through an Ethernet port is faster than through the console port.

Prerequisites

Make sure that the prerequisites are met before you start upgrading software from the Boot menu.

Upgrading environment

Use a console cable to connect the console terminal, for example, a PC, to the console port on the switch. Run a terminal emulator program on the console terminal and set the following terminal settings:

- **Bits per second**—9,600
- **Data bits**—8
- **Parity**—None
- **Stop bits**—1
- **Flow control**—None
- **Emulation**—VT100

TFTP/FTP download

To use TFTP or FTP:

- Run a TFTP or FTP server program on the file server or the console terminal.
- Copy the upgrade file to the file server.
- Correctly set the working directory on the TFTP or FTP server.
- Make sure that the file server and the switch can reach each other.

Storage space

Make sure that sufficient space is available for the upgrading software file. If no sufficient space is available, delete obsolete files as described in "Managing files from the Boot menu."

Upgrading time

Make sure that the upgrade has minimal impact on the network services. During the upgrade, the switch cannot provide any services.

Accessing the Boot menu

Power on the switch (for example, an HPE FF 5940-32QSFP+ Switch), and you can see the following information:

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU...
Press Ctrl+T to start heavy memory test

**************************************************************************
*                                                                        *
*              HPE FF 5940-32QSFP+ Switch BOOTROM, Version 205            *
*                                                                        *
**************************************************************************
Copyright (c) 2010-2016 Hewlett-Packard Development Company, L.P.
```

```
Creation Date   : Jan  6 2013, 14:25:58
CPU Clock Speed : 1000MHz
Memory Size     : 4096MB
Flash Size      : 1024MB
CPLD Version    : 002/002
PCB Version     : Ver.A
Mac Address     : 00E0FC005800


Press Ctrl+B to access EXTENDED BOOT MENU...1
```

Press one of the shortcut key combinations at prompt.

Table 8 Shortcut keys

Shortcut keys	Prompt message	Function	Remarks
Ctrl+B	Press Ctrl+B to enter Extended Boot menu...	Accesses the extended Boot menu.	Press the keys within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the message appears. You can upgrade and manage system software and Boot ROM from this menu.
Ctrl+D	Press Ctrl+D to access BASIC BOOT MENU	Accesses the basic Boot menu.	Press the keys within 1 seconds after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.
Ctrl+T	Press Ctrl+T to start heavy memory test	Performs a RAM pressure test.	Press the keys within 1 second after the message appears.

Accessing the basic Boot menu

If the extended Boot ROM segment has corrupted, you can repair or upgrade it from the basic Boot menu.

Press **Ctrl+D** within 1 seconds after the "Press Ctrl+D to access BASIC BOOT MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended Boot ROM segment.

```
********************************************************************************
*                                                                              *
*                            BASIC BOOTROM, Version 205                        *
*                                                                              *
********************************************************************************


   BASIC BOOT MENU

1. Update full BootRom
2. Update extended BootRom
```

```
3. Update basic BootRom
4. Boot extended BootRom
0. Reboot
Ctrl+U: Access BASIC ASSISTANT MENU

Enter your choice(0-4):
```

Table 9 Basic Boot ROM menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
2. Update extended BootRom	Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
3. Update basic BootRom	Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see Accessing the extended Boot menu.
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press **Ctrl + U** to access the BASIC ASSISTANT menu (see Table 10).

Table 10 BASIC ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.
0. Return to boot menu	Return to the basic Boot menu.

Accessing the extended Boot menu

Press **Ctrl+B** within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the "Press Ctrl-B to enter Extended Boot menu..." prompt message appears. If you fail to do this, the system starts decompressing the system software.

Alternatively, you can enter **4** in the basic Boot menu to access the extended Boot menu.

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 11). For more information about password recovery capability, see *HPE FlexFabric 5940 Switch Series Fundamentals Configuration Guide*.

```
Password recovery capability is enabled.

   EXTENDED BOOT MENU

1. Download image to flash
```

```
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8):
```

Table 11 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	• Specify the main and backup software image file for the next startup. • Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+Y: Change the operating mode	If PEX mode is enabled, the operation disables PEX mode. If PEX mode is disabled, the operation enables PEX mode.
Ctrl+R: Download image to SDRAM and run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.

Option	Tasks
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 12.

Table 12 EXTENDED ASSISTANT menu options

Option	Task
1. Display Memory	Display data in the memory.
2. Search Memory	Search the memory for a specific data segment.
0. Return to boot menu	Return to the extended Boot ROM menu.

Using TFTP to upgrade software images through the management Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 13 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu, enter **N**.

```
Loading.....................................................................
.............................................................................
.............................................................................
.....................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash...............................................................
.............................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash...............................................................
.............................................................................
.............................................................................
.............................................................................
.............................................................................
.............................................................................
.....................................................Done!
```

NOTE:

- The switch always attempts to boot first with the main images, and if the attempt fails, for example, because the main images are not available, the switch tries to boot with the backup images. An image with the none attribute is just stored in Flash memory for backup and you must change its attribute to make it usable at reboot.
- If an image with the same attribute as the image you are loading is already in Flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8):0
```

Using FTP to upgrade software through the management Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **2** to set the FTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
FTP User Name       :switch
FTP User Password   :***
```

Table 14 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu, enter **N**.

```
Loading.....................................................................
.............................................................................
.............................................................................
.............................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
```

```
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash.....................................................................
.....................................................................................
.....................................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................Done!

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8):0
```

NOTE:

- The switch always attempts to boot first with the main images, and if the attempt fails, for example, because the main images not available, the switch tries to boot with the backup images. An image with the none attribute is just stored in Flash memory for backup and you must change its attribute to make it usable at reboot.
- If an image with the same attribute as the image you are loading is already in Flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

Using XMODEM to upgrade software through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the management Ethernet port. To save time, use the management Ethernet port as long as possible.

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **3** to set the XMODEM download baud rate.

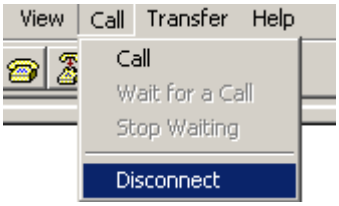
```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

Enter your choice(0-5):5
```

3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

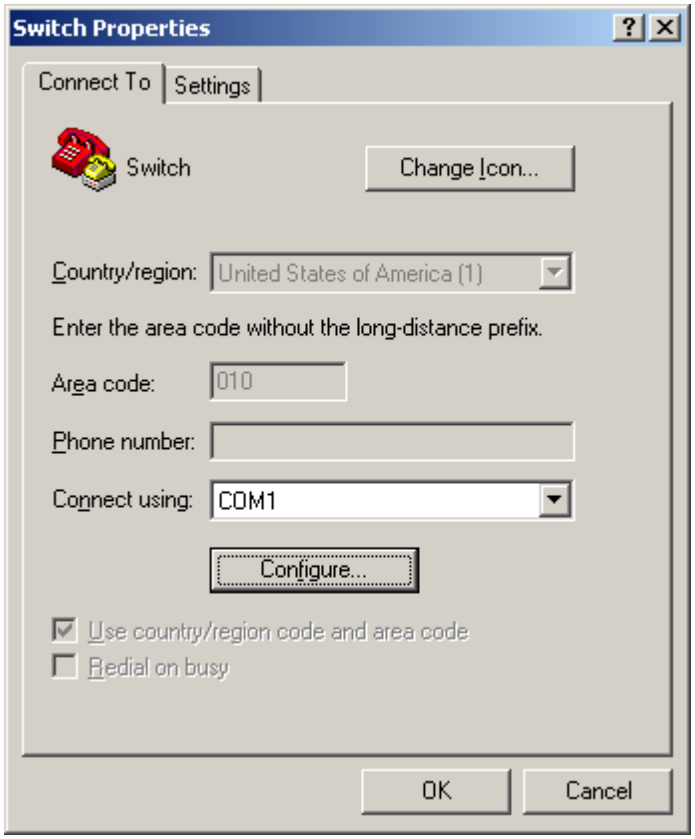
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
5. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



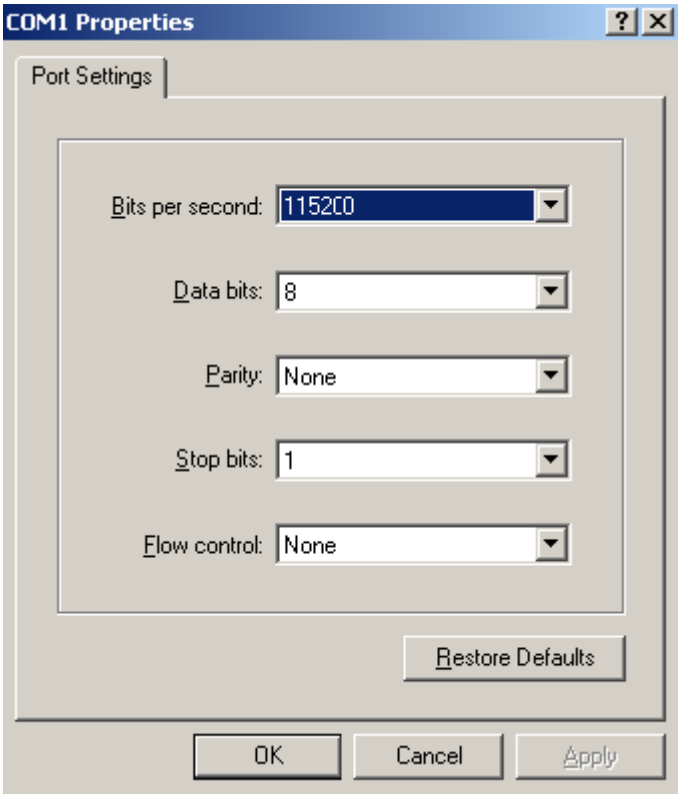
6. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



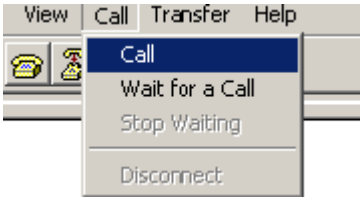
7. Select **115200** from the **Bits per second** list and click **OK**.

Figure 4 Modifying the baud rate



8. Select **Call** > **Call** to reestablish the connection.

Figure 5 Reestablishing the connection



9. Press **Enter**. The following prompt appears:

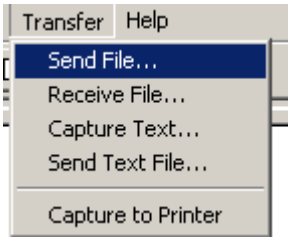
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

10. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCC
```

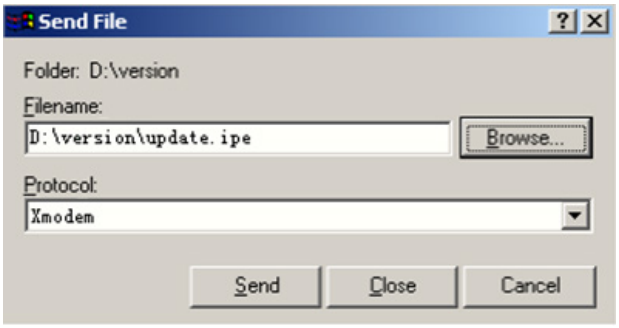
11. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 6 Transfer menu



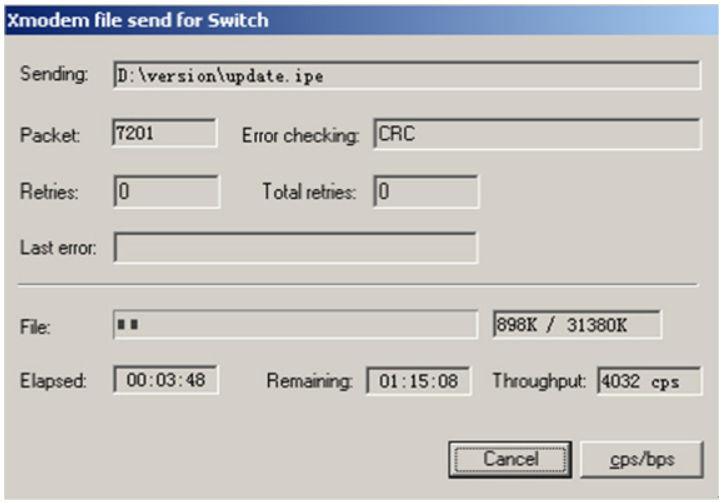
12. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box



13. Click **Send**. The following dialog box appears:

Figure 8 File transfer progress



14. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
At the Load File name prompt, enter a name for the Boot image to be saved to Flash memory.
Load File name  : default_file boot-update.bin
Free space: 470519808 bytes
Writing flash.....................................................................
.............Done!
The system-update.bin image is self-decompressing...
At the Load File name prompt, enter a name for the system image to be saved to Flash memory.
Load File name  : default_file system-update.bin
Free space: 461522944 bytes
Writing flash.....................................................................
.............Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

NOTE:

- The switch always attempts to boot first with the main images, and if the attempt fails, for example, because the main images not available, the switch tries to boot with the backup images. An image with the none attribute is just stored in Flash memory for backup and you must change its attribute to make it usable at reboot.
- If an image with the same attribute as the image you are loading is already in Flash memory, the attribute of the old image changes to none after the new image becomes valid.

15. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps. If the baud rate is 9600 bps, skip this step.

To access the switch through the console port after a reboot, you must perform this step, because the console port rate reverts to 9600 bps at a reboot.

16. Press **Enter** to access the Boot menu.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8):0
```

17. Enter **0** to reboot the system with the new software images.

Using TFTP to upgrade Boot ROM through the management Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
```

```
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.btm
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 15 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.
- If .bin files are used for upgrade, specify the .bin files in the order of the boot image, system image, and feature images. If you specify a .bin file for a feature image before the .bin file for the system image or the boot image, the upgrade might fail

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.............................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using FTP to upgrade Boot ROM through the management Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **2** to set the FTP parameters.

```
Load File Name     :update.btm
Server IP Address  :192.168.0.3
Local IP Address   :192.168.0.2
Subnet Mask        :255.255.255.0
Gateway IP Address :0.0.0.0
FTP User Name      :switch
FTP User Password  :***
```

Table 16 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.
- If .bin files are used for upgrade, specify the .bin files in the order of the boot image, system image, and feature images. If you specify a .bin file for a feature image before the .bin file for the system image or the boot image, the upgrade might fail

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.....................................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
```

```
Updating Basic BootRom..........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using XMODEM to upgrade Boot ROM through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the management Ethernet port. To save time, use the management Ethernet port as long as possible.

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **3** to set the XMODEM download baud rate.

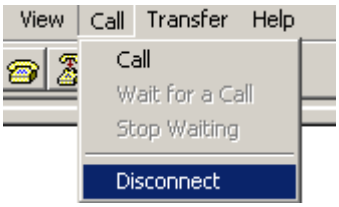
```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

Enter your choice(0-5):5
```

4. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

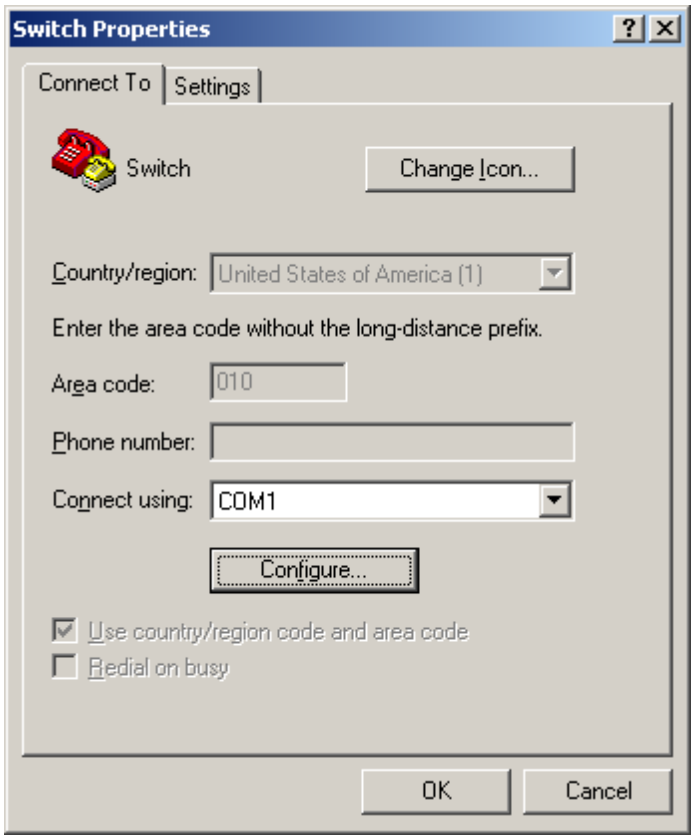
5. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
6. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



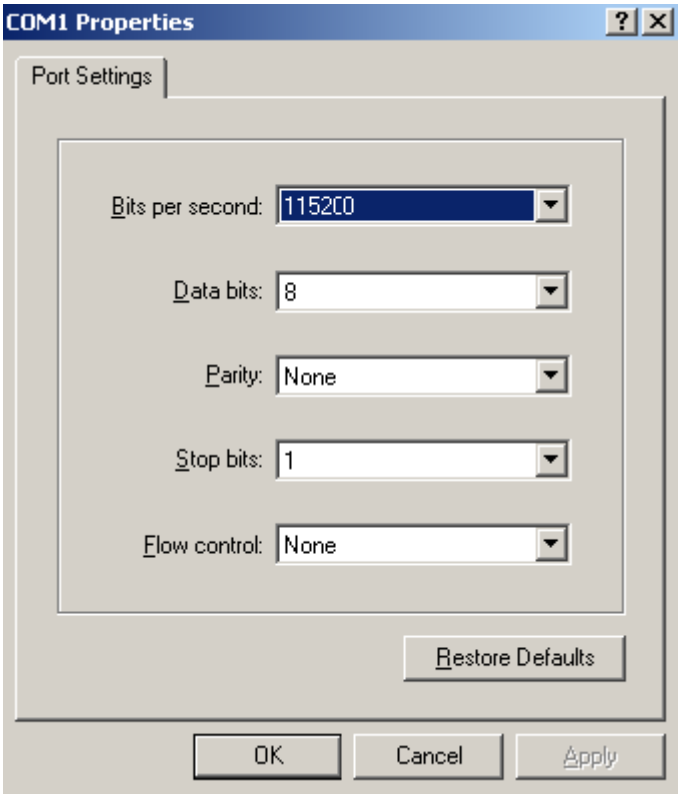
7. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



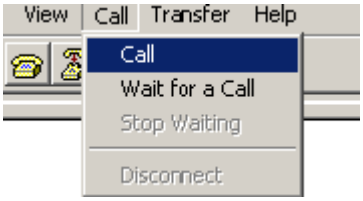
8. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



9. Select **Call** > **Call** to reestablish the connection.

Figure 12 Reestablishing the connection

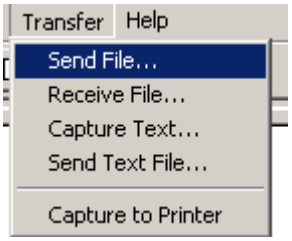


10. Press **Enter** to start downloading the file.

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCC
```

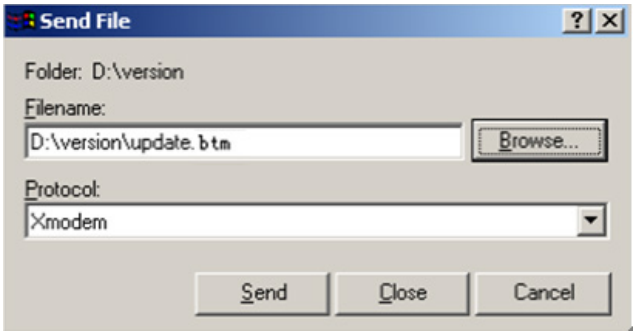
11. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



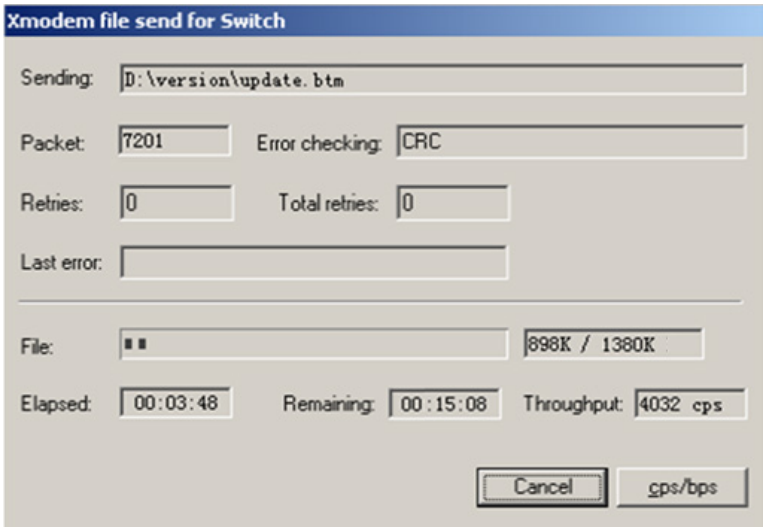
12. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 14 File transmission dialog box



13. Click **Send**. The following dialog box appears:

Figure 15 File transfer progress



14. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Loading ...CCCCCCCCCCCCC  ...Done!
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom...........Done.
```

15. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

16. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps at the prompt. If the baud rate is 9600 bps, skip this step.

```
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.
```

To access the switch through the console port after a reboot, you must perform this step, because the console port rate reverts to 9600 bps at a reboot.

17. Press **Enter** to access the Boot ROM update menu.

18. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

19. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Managing files from the Boot menu

From the Boot menu, you can display files in Flash memory to check for obsolete files, incorrect files, or space insufficiency, delete files to release storage space, or change the attributes of software images.

Displaying all files

Enter **3** in the Boot menu to display all files in Flash memory and identify the free space size.

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8): 3
```

The following is a sample output:

```
Display all file(s) in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
4              3678                 flash:/startup.cfg_backup
5              30033                flash:/default.mdb
6              42424                flash:/startup.mdb
7              18                   flash:/.pathfile
8              232311               flash:/logfile/logfile.log
9              5981                 flash:/startup.cfg_back
10(*)          6098                 flash:/startup.cfg
11             20                   flash:/.snmpboots
Free space: 1009906637 bytes
The current image is boot.bin
(*)-with main attribute
```

```
(b)-with backup attribute
(*b)-with both main and backup attribute
```

Deleting files

If storage space is insufficient, delete obsolete files to free up storage space.

To delete files:

1. Enter **4** in the Boot menu:

```
Deleting the file in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
4              3678                 flash:/startup.cfg_backup
5              30033                flash:/default.mdb
6              42424                flash:/startup.mdb
7              18                   flash:/.pathfile
8              232311               flash:/logfile/logfile.log
9              5981                 flash:/startup.cfg_back
10(*)          6098                 flash:/startup.cfg
11             20                   flash:/.snmpboots
Free space: 1009906637 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

2. Enter the number of the file to delete. For example, enter **1** to select the file **testbackup.cfg**.

```
Please input the file number to change: 1
```

3. Enter **Y** at the confirmation prompt.

```
The file you selected is testbackup.cfg,Delete it? (Y/N):Y
Deleting.................................Done!
```

Changing the attribute of software images

Software image attributes include main (M), backup (B), and none (N). System software and boot software can each have multiple none-attribute images but only one main image and one backup image on the switch. You can assign both the M and B attributes to one image. If the M or B attribute you are assigning has been assigned to another image, the assignment removes the attribute from that image. If the removed attribute is the sole attribute of the image, its attribute changes to N.

For example, the system image **system.bin** has the M attribute and the system image **system-update.bin** has the B attribute. After you assign the M attribute to **system-update.bin**, the attribute of **system-update.bin** changes to M+B and the attribute of **system.bin** changes to N.

To change the attribute of a system or boot image:

1. Enter **2** in the Boot menu.

```
   EXTENDED BOOT MENU
```

```
1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+Y: Change Work Mode
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8): 2
```

2. Enter **1** or **2** at the prompt to set the attribute of a software image. (The following output is based on the option **2**. To set the attribute of a configuration file, enter **3**.)

```
1. Set image file
2. Set bin file
3. Set configuration file
0. Return to boot menu

Enter your choice(0-3): 2

File Number    File Size(bytes)     File Name
================================================================================
1(*)              53555200              flash:/system.bin
2(*)              9959424              flash:/boot.bin
3                 13105152              flash:/boot-update.bin
4                 91273216             flash:/system-update.bin
Free space: 905848832 bytes
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Note:Select .bin files. One but only one boot image and system image must be included.
```

3. Enter the number of the file you are working with. For example, enter **3** to select the boot image **boot-update.bin** and enter **4** to select the system image **system-update.bin**.

```
Enter file No.(Allows multiple selection):3
Enter another file No.(0-Finish choice):4
```

4. Enter **0** to finish the selection.

```
Enter another file No.(0-Finish choice):0
You have selected:
flash:/boot-update.bin
flash:/system-update.bin
```

5. Enter **M** or **B** to change its attribute to main or backup. If you change its attribute to M, the attribute of **boot.bin** changes to none.

```
Please input the file attribute (Main/Backup) M
```

```
This operation may take several minutes. Please wait....
Next time, boot-update.bin will become default boot file!
Next time, system-update.bin will become default boot file!
Set the file attribute success!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version.

To handle a software upgrade failure:

1. Verify that the software release is compatible with the switch model and the correct file is used.
2. Verify that the software release and the Boot ROM release are compatible. For software and Boot ROM compatibility, see the hardware and software compatibility matrix in the correct release notes.
3. Check the physical ports for a loose or incorrect connection.
4. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
5. Check the file transfer settings:
   - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
   - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
   - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.
6. Check the FTP or TFTP server for any incorrect setting.
7. Check that the storage device has sufficient space for the upgrade file.

Hewlett Packard Enterprise

HPE 5710-CMW710-R6710P03 Release Notes

Software Feature Changes

Contents

About software feature changes

This document contains feature changes in the software versions listed in Table 1. For information about software feature changes in HPE 5710-CMW710-F2708 (or earlier), see their respective release notes (software feature changes).

Table 1 Software feature change summary

Section	Software feature changes
Release 6710P01	Contains changes in HPE 5710-CMW710-R6710P01 over HPE 5710-CMW710-R6710.
Release 6710	Contains changes in HPE 5710-CMW710-R6710 over HPE 5710-CMW710-F6702.
Feature 6702	Contains changes in HPE 5710-CMW710-F6702 over HPE 5710-CMW710-F2708.

Release 6710P03

This release has the following changes:

- New feature: DRNI configuraton
- New feature: Generating a log message to display product version numbers before and after a software upgrade

New feature: DRNI configuraton

All DRNI commands were newly added.

New feature: Generating a log message to display product version numbers before and after a software upgrade

Generating a log message to display product version numbers before and after a software upgrade

As from this version, the device can generate a log message to display the product version numbers before and after a software upgrade when it successfully upgrades the software by executing the **`install`**, **`issu`**, or **`boot-loader`** command.

Log message reference

PKG_UPGRADE_INFO

Message text	The [STRING] device upgraded the software version from [STRING] to software [STRING].
Variable fields	$1: Device name. $2: Version number before software upgrade. $3: Version number after software upgrade.
Severity level	5 (Notification)
Example	PKG/5/PKG_UPGRADE_INFO: The HPE FF 5710 48SFP+ 6QSFP+ or 2QSFP28 Switch device upgraded the software version from software version 1-patch version 1 to software version 2-patch version 2.
Impact	No negative impact on the system.
Cause	Executed the **`install`**, **`issu`**, or **`boot-loader`** command successfully and the new version took effect.
Recommended action	No action is required.

Release 6710

This release has the following changes:

- New features: Fundamentals features
- New features: Layer 2—LAN switching features
- New features: Layer 3—IP services features
- New features: Layer 3—IP routing features
- New features: IP multicast features
- New features: ACL and QoS features
- New features: Security features
- New features: High availability features
- New features: Network management and monitoring features
- New features: Telemetry features
- New features: OpenFlow features
- New features: VXLAN features
- New features: Intelligent lossless network features
- New features: M-LAG support for DRNI commands
- New feature: FEC mode
- New feature: Displaying ND entry statistics
- New feature: User IP address conflict SNMP notifications for ARP
- New feature: Interface alarm functions
- New feature: Advertising only the global unicast address in the NEXT_HOP attribute
- New feature: IPv6 duplicate detection on duplicate addresses
- New feature: BGP route re-origination
- New feature: Establishing neighbors through the secondary IP address of an interface
- Modified feature: IPv6 routes with prefixes longer than 64 bits
- Modified feature: Match criteria in a traffic class
- Modified feature: Associating a traffic behavior with a traffic class
- Modified feature: Displaying the running configuration
- Modified feature: Displaying the contents of the configuration file for the next system startup
- Modified feature: Optimized display of BGP BMP server information
- Modified feature: Disabling BGP session establishment with peers and peer groups
- Modified feature: Optimizations to VXLAN command output
- Modified feature: Sharing of VSI interfaces among VSIs
- Modified feature: Enabling L2TP for the specified protocol
- Modified feature: Creating a local site
- Modified feature: Enabling link flapping protection on an interface
- Modified feature: AAA methods in an ISP domain
- Modified feature: Setting the 802.1X periodic reauthentication timer
- Modified feature: Setting the periodic MAC reauthentication timer
- Modified feature: Creating an SNMPv3 user

- Modified feature: Displaying local public keys
- Modified feature: Flow-mirroring traffic to an interface
- Modified feature: Disabling the device from learning the source MAC addresses of Layer 2 protocol packets
- Modified feature: Specifying multiple VLAN IDs for VLAN name TLVs
- Modified feature: Applying a QoS policy to an interface
- Modified feature: Configuring MAC address borrowing
- Modified feature: Configuring the types of advertisable TLVs on a port
- Modified feature: DRNI term changes

New features: Fundamentals features

Table 1 describes the fundamentals features added in this software version.

For more information about the features, see *Fundamentals Configuration Guide* in in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Fundamentals Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 1 Fundamentals features in Release 6710

Feature	Command changes
Login management: Controlling TCP connections from IPv6 HTTP and HTTPS clients.	The following commands were added: • **`http ipv6 acl`** • **`https ipv6 acl`**
Login management: Specifying the service port number for RESTful access over HTTP/HTTPS.	The following commands were added: • **`restful http port`** • **`restful https port`**
Login management: Applying an SSL server policy to the RESTful access over HTTPS service.	The **`restful https ssl-server-policy`** command was added.
FTP and TFTP: Enabling the TFTP server.	The **`tftp server enable`** command was added.
FTP and TFTP: Setting the TFTP server working directory.	The **`tftp server work-directory`** command was added.
Configuration file management: Assigning a user exclusive write access to the configuration.	The following commands were added: • **`configuration exclusive by-user-name`** • **`display configuration exclusive by-user-name`**
Device management: Displaying the historical power consumption information in a coordinate system.	The **`display power history`** command was added.
Device management: Displaying system health status information.	The **`display system health`** command was added.
Device management: Displaying historical system health status change information.	The **`display system health history`** command was added.
Device management: Enabling periodic CPU usage logging.	The **`monitor cpu-usage logging interval`** command was added.

Feature	Command changes
Device management: Enabling periodic memory usage logging.	The **monitor memory-usage logging interval** command was added.
Device management: Configuring error notifications for software and hardware table entry consistency check.	The following commands were added: • **parity-error consistency-check log enable** • **parity-error consistency-check threshold**
Device management: Configuring unrecoverable error notifications for critical hardware entry parity check and ECC check.	The following commands were added: • **parity-error unrecoverable log enable** • **parity-error unrecoverable period** • **parity-error unrecoverable reboot** • **parity-error unrecoverable threshold**
Device management: Enabling transceiver monitoring.	The following commands were added: • **transceiver monitor enable** • **transceiver monitor interval**
Device management: Displaying or saving IFMGR-related operating information.	The **ifmgr** keyword was added to the **display diagnostic-information** command.
GIR features	All GIR commands were newly added.

New features: Layer 2—LAN switching features

Table 2 describes the Layer 2—LAN switching features added in this software version.

For more information about the features, see *Layer 2—LAN Switching Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Layer 2—LAN Switching Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 2 Layer 2—LAN switching features added in Release 6710

Feature	Command changes
Ethernet interface: Displaying the physical link state change statistics of interfaces	The **display link-state-change statistics interface** command was added.
Ethernet interface: Clearing the physical link state change statistics of interfaces	The **reset link-state-change statistics interface** command was added.
Ethernet interface: Configuring alarm parameters for sent or received pause frames	The following commands were added: • **ifmonitor input-usage** • **ifmonitor output-usage** • **ifmonitor rx-pause** • **ifmonitor tx-pause** • **port ifmonitor input-usage** • **port ifmonitor output-usage** • **port ifmonitor rx-pause** • **port ifmonitor tx-pause**

Feature	Command changes
Ethernet interface: Shutting down all physical interfaces except the management Ethernet interfaces	The **shutdown all-physical-interfaces** command was added.
VLAN: Configuring the 802.1p priority for control packets sent by the device	The **control-packet dot1p** *priority* command was added.
VLAN mapping: Configuring many-to-one VLAN mapping in the IPv6 address environment	None.
Loop detection: Setting the loop protection delay timer	The following commands were added: • **loopback-detection global delay-timer** *time* • **loopback-detection delay-timer** *time*
Loop detection: Configuring loop detection in a VXLAN network	The following commands were added: • **display loopback-detection** • **loopback-detection action** { **block** | **shutdown** } • **loopback-detection enable** [**vlan** *vlan-id-list*] • **loopback-detection enable s-vid** *vlan-id-list* **c-vid** *vlan-id-list* • **loopback-detection interval-time** *interval* • **loopback-detection priority** *priority*
Spanning tree: Enabling BPDU filter	The following commands were added: • **stp bpdu-filter** • **stp port bpdu-filter** { **disable** | **enable** }
Spanning tree: Enabling loopback guard on an interface	The **stp loopback-protection** command was added.
LLDP: Setting the port ID subtype of port ID TLVs advertised by LLDP on a device	The **lldp tlv-config basic-tlv port-id** *type-id* command was added.
Ethernet link aggregation: Displaying the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state	The **display link-aggregation troubleshooting** command was added.
Ethernet link aggregation: Enabling automatic link aggregation	The **link-aggregation auto-aggregation enable** command was added.
Ethernet link aggregation: Isolating aggregate interfaces on the device	The **link-aggregation lacp isolate** command was added.
Ethernet link aggregation: Configuring LACP system settings on an aggregate interface	The following commands were added: • **port lacp system-mac** • **port lacp system-priority**
Ethernet link aggregation: Displaying information about all member ports in an aggregation group	The **all-configuration** keyword was added to the **display link-aggregation verbose** command.

Feature	Command changes
M-LAG: Displaying the configuration consistency check status	The **display m-lag consistency-check status** command was added.
M-LAG: Displaying M-LAG troubleshooting information	The **display m-lag troubleshooting** command was added.
M-LAG: Enabling M-LAG packet authentication and configuring an authentication key	The **m-lag authentication key** command was added.
M-LAG: Setting the mode of configuration consistency check	The **m-lag consistency-check mode** command was added.
M-LAG: Configuring M-LAG extra VLANs	The **m-lag extra-vlan** command was added.
M-LAG: Enabling the peer-link interface to retain MAC address entries for single-homed devices	The **m-lag peer-link mac-address hold** command was added.
M-LAG: Associating the keepalive link with a track entry	The **m-lag keepalive track** command was added.
M-LAG: Excluding all logical interfaces from the shutdown action by M-LAG MAD	The **m-lag mad exclude logical-interfaces** command was added.
M-LAG: Enabling M-LAG MAD DOWN state persistence	The **m-lag mad persistent** command was added.
M-LAG: Bringing up the interfaces in M-LAG MAD DOWN state	The **m-lag mad restore** command was added.
M-LAG: Enabling M-LAG sequence number check	The **m-lag sequence enable** command was added.
M-LAG: Enabling M-LAG standalone mode	The **m-lag standalone enable** command was added.
M-LAG: Clearing M-LAG troubleshooting records	The **reset m-lag troubleshooting history** command was added.
M-LAG: Configuring dynamic routing access to M-LAG	The following commands were added: • **port m-lag virtual-ip** • **port m-lag ipv6 virtual-ip** • **display m-lag virtual-ip**
M-LAG: Configuring M-LAG system settings on an aggregate interface	The following commands were added: • **port m-lag system-priority** • **port m-lag system-mac**

New features: Layer 3—IP services features

Table 3 describes the Layer 3 IP services features added in this software version.

- For more information about the features, see *Layer 3—IP services Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.
- For more information about the commands, see *Layer 3—IP services Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 3 Layer 3 IP services features added in Release 6710

Feature	Command changes
ARP: Enabling error logging for ARP entry deployment to hardware	The **arp hardware log enable** command was added.
ARP: Displaying the ARP table usage	The **display arp usage** command was added.
ARP: Displaying statistics about proxy ARP reply packets	The **display proxy-arp statistics** command was added.
ARP: Displaying information about ARP direct route advertisement	The **display arp route-direct advertise** command was added.
ARP: Enabling dropping ARP requests that match FIB entries	The **arp fib-miss drop** command was added.
ARP: Testing whether an IPv4 address in a LAN is being used by sending ARP requests	The **ping arp ip** command was added.
ARP: Testing whether a MAC address exists in a specified network or to view its corresponding IPv4 address	The **ping arp mac** command was added.
DHCP: Enabling IP exhaustion event logging	The **exhaustion log enable** command was added.
DHCP: Enabling IP exhaustion notifications for an IP pool	The **exhaustion trap enable** command was added.
DHCP: Enabling SNMP notifications for the DHCP server	The **snmp-agent trap enable dhcp server** command was added.
DHCP: Specifying the IP address to be filled in sub-option 5 of Option 82	The **dhcp relay information link-selection** command was added.
DHCP: Enabling release notification	The **dhcp relay release-agent** command was added.
DHCP: Enabling packet drop alarm logging	The following commands were added: . **dhcp snooping alarm enable** (system view) . **dhcp snooping alarm enable** (interface view)
DHCP: Setting a packet drop alarm threshold	The following commands were added: . **dhcp snooping alarm threshold** (system view) . **dhcp snooping alarm threshold** (interface view)
DHCP: Enabling the **giaddr** field check in DHCP requests	The **dhcp snooping check giaddr** command was added.
DHCP: Enabling client offline detection	The **dhcp snooping client-detect** command was added.
DHCP: Enabling DHCP snooping entry exhaustion notifications	The **dhcp snooping exhaustion trap enable** command was added.
DHCP: Setting the DHCP snooping entry usage threshold	The **dhcp snooping learning-num-threshold** command was added.
DHCP: Enabling recording untrusted DHCP servers	The **dhcp snooping untrusted-server-record enable** command was added.
DHCP: Displaying statistics for dropped DHCP packets on an interface of the DHCP snooping device	The **display dhcp snooping alarm packet statistics** command was added.

Feature	Command changes
DHCP: Displaying statistics about the packets exchanged between M-LAG member devices for DHCP snooping entry synchronization	The **display dhcp snooping m-lag-statistics** command was added.
DHCP: Displaying M-LAG status information	The **display dhcp snooping m-lag-status statistics** command was added.
DHCP: Clearing statistics for dropped DHCP packets on a DHCP snooping device	The **reset dhcp snooping alarm packet statistics** command was added.
DHCP: Clearing statistics about the packets exchanged between M-LAG member devices for DHCP snooping entry synchronization	The **reset dhcp snooping m-lag-statistics** command was added.
DHCP: Enabling SNMP notifications for DHCP snooping events	The **snmp-agent trap enable dhcp snooping** command was added.
IP forwarding basics: Enabling SNMP notifications for FIB events	The **snmp-agent trap enable fib** command was added.
IP forwarding basics: Displaying the FIB table usage	The **display fib usage** command was added.
IP performance optimization: Enabling the device to respond to broadcast echo requests	The **ip icmp broadcast-echo-reply enable** command was added.
IP performance optimization: Enabling the device to send a specific type of ICMP messages	The **ip icmp send enable** command was added.
IP performance optimization: Enabling the device to receive a specific type of ICMP messages	The **ip icmp receive enable** command was added.
IP performance optimization: Enabling SNMP notifications for TCP events	The **snmp-agent trap enable tcp** command was added.
ARP: Configuring the description for a static ARP entry	The [**description** *text*] option was added to the **arp static** command.
ARP: Configuring the description for a multiport ARP entry	The [**description** *text*] option was added to the **arp multiport** command.
ARP: Displaying detailed information about ARP entries for a VPN instance	The **verbose** keyword was added to the **display arp vpn-instance** command.
ARP: Setting the preference and route tag for ARP-advertised direct routes	The **preference** *preference-value* and **tag** *tag-value* options were added to the **arp route-direct advertise** command.
DHCP: Retaining the original address in the **giaddr** field in relayed DHCP requests	The **default-giaddr** keyword was added to the **dhcp relay source-address** command.
Tunneling: Enabling SNMP notifications for tunneling	The **snmp-agent trap enable tunnel [vxlan-tunnel-status | vxlan-ipv6-tunnel-status] *** command was added.
IPv6 basics: Displaying complete IPv6 interface descriptions	The **description** keyword was added to the **display ipv6 interface** command.

Feature	Command changes
IPv6 basics: Displaying statistics for ND proxy reply packets	The **display ipv6 nd proxy statistics** command was added.
IPv6 basics: Displaying information about ND direct route advertisement	The **display ipv6 nd route-direct advertise interface** *interface-type interface-number* command was added.
IPv6 basics: Displaying the ND table usage	The **display ipv6 neighbors usage** command was added.
IPv6 basics: Dropping the NS packets whose destination addresses already exist in the FIB table	The **ipv6 nd fib-miss drop** command was added.
IPv6 basics: Enabling logging ND entry deployment events	The **ipv6 nd hardware log enable** [**count-limit** *count-limit-value*] command was added.
IPv6 basics: Configuring a static neighbor entry	The following options were added to the **ipv6 neighbor** command: • **vsi-interface** *vsi-interface-id* • **tunnel** *number* • **vsi** *vsi-name* • **service-instance** *instance-id*
IPv6 basics: Setting the maximum number of probes to test the reachability of neighbors in ND entries	The **ipv6 neighbor aging probe-count** *count* command was added.
IPv6 basics: Setting the interval for testing the reachability of neighbors in ND entries.	The **ipv6 neighbor aging probe-interval** *interval* command was added.
IPv6 basics: Verifying the availability of an IPv6 address in the LAN	The **ping nd ipv6** *host* [**interface** *interface-type interface-number* [**vlan** *vlan-id*]] [**timeout** *timeout*] [**count** *count*] command was added.
IPv6 basics: Obtaining the IPv6 address of the device that uses the specified MAC address in a specific subnet	The **ping nd mac** *mac-address* { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] } [**timeout** *timeout*] [**count** *count*] command was added.
DHCPv6: Enabling IPv6 resource exhaustion logging	The **exhaustion log enable** command was added.
DHCPv6: Enabling IPv6 resource exhaustion alarming for an IPv6 address pool	The **exhaustion trap enable** command was added.
DHCPv6: Setting the IPv6 address usage threshold for an IPv6 address pool	The **ip-in-use threshold** *threshold-value* command was added.
DHCPv6: Setting the prefix usage threshold for an IPv6 address pool	The **pd-in-use threshold** *threshold-value* command was added.
DHCPv6: Enabling SNMP notifications for the DHCPv6 server	The **snmp-agent trap enable ipv6 dhcp server** [**address-exhaust** | **ip-in-use | pd-exhaust | pd-in-use**] * command was added.
DHCPv6: Configuring a suboption for a DHCPv6 vendor-specific option	The **suboption** *suboption-code* { **address** *ipv6-address*&<1-4> | **ascii** *ascii-string* |

Feature	Command changes
(Option 17)	**hex** *hex-string* } command was added.
DHCPv6: Configuring a DHCPv6 vendor-specific option for an IPv6 address pool and enter the option view	The **vendor-specific** *vendor-id* command was added.
DHCPv6: Setting the aging timer for DUID entries on a DHCPv6 relay interface	The **ipv6 dhcp relay duid aging-time** *seconds* command was added.
DHCPv6: Specifying the DUID to be set in Option 37	The **ipv6 dhcp relay remote-id duid** { **ascii** *ascii-string* | **hex** *hex-string* } command was added.
DHCPv6: Enabling the DHCPv6 relay agent to add Option 37 in Relay-forward messages	The **ipv6 dhcp relay remote-id enable** command was added.
DHCPv6: Configuring the DHCPv6 relay agent to discard the DHCPv6 requests that are delivered from VXLAN tunnels	The **ipv6 dhcp relay request-from-tunnel discard** command was added.
DHCPv6: Configuring smart relay on a DHCPv6 relay interface	The **ipv6 dhcp smart-relay** { **count** *count* | **time** *seconds* } * command was added.
DHCPv6: Enabling smart relay on a DHCPv6 relay interface	The **ipv6 dhcp smart-relay enable** command was added.
DHCPv6: Enabling the packet drop alarm	The **ipv6 dhcp snooping alarm** { **relay-forward** | **request-message** } **enable** command was added.
DHCPv6: Setting a packet drop alarm threshold	The **ipv6 dhcp snooping alarm** { **relay-forward** | **request-message** } **threshold** *threshold* command was added.
DHCPv6: Enabling support for the interface-ID option (also called Option 18)	The **ipv6 dhcp snooping option interface-id enable** command was added.
DHCPv6: Enabling the lightweight DHCPv6 relay agent (LDRA) on an interface	The **ipv6 dhcp snooping relay-agent enable** [**trust**] command was added.

New features: Layer 3—IP routing features

Table 4 describes the Layer 3 IP services features added in this software version.

For more information about the features, see *Layer 3—IP Routing Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Layer 3—IP Routing Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 4 Layer 3 IP routing features added in Release 6710

Feature	Command changes
OSPF: Displaying OSPF neighbor relationship troubleshooting information	The **display ospf troubleshooting** command was added.

Feature	Command changes
OSPF: Enabling OSPF isolation	The **isolate enable** command was added.
OSPF: Associating an OSPF interface with a track entry to adjust the cost of the interface based on the track entry state.	The **ospf track adjust-cost** command was added.
OSPF: Setting the maximum number of OSPF neighbor relationship troubleshooting entries	The **ospf troubleshooting max-number** command was added.
OSPF: Clearing OSPF neighbor relationship troubleshooting information	The **reset ospf troubleshooting** command was added.
OSPF: Shutting down an OSPF process	The **shutdown process** command was added.
IS-IS: Displaying IS-IS log information about received or sent hello packets	The **display isis event-log hello** command was added.
IS-IS: Displaying neighbor state change log information	The **display isis event-log peer** command was added.
IS-IS: Displaying information about the first three and last three packets sent by an interface	The **display isis interface hello-sent** command was added.
IS-IS: Displaying information about hello packets received from neighbors	The **display isis peer hello-received** command was added.
IS-IS: Displaying IS-IS neighbor relationship troubleshooting information	The **display isis troubleshooting** command was added.
IS-IS: Setting the maximum number of log entries that IS-IS can record	The **event-log size** command was added.
IS-IS: Setting the maximum cost from the source node of a protected link to a PQ node	The **fast-reroute remote-lfa maximum-cost** command was added.
IS-IS: Specifying a prefix list to filter remote LFA PQ nodes	The **fast-reroute remote-lfa prefix-list** command was added.
IS-IS: Enabling IS-IS remote Loop-free Alternate (LFA) FRR	The **fast-reroute remote-lfa tunnel ldp** command was added.
IS-IS: Setting the priority for a backup path selection policy	The **fast-reroute tiebreaker** command was added.
IS-IS: Disabling remote LFA calculation on an interface	The **isis fast-reroute remote-lfa disable** command was added.
IS-IS: Setting the maximum number of IS-IS neighbor relationship troubleshooting entries	The **isis troubleshooting max-number** command was added.
IS-IS: Enabling IS-IS isolation	The **isolate enable** command was added.
IS-IS: Enabling the IS-IS	The **multi-instance enable** command was added.

Feature	Command changes
multi-instance process and specify an instance ID for the process	
IS-IS: Clearing IS-IS GR log information	The **reset isis event-log graceful-restart** command was added.
IS-IS: Clearing IS-IS neighbor relationship troubleshooting information	The **reset isis troubleshooting** command was added.
IS-IS: Shutting down an IS-IS process	The **shutdown process** command was added.
IS-IS: Generating notifications about IS-IS address family changes and IS-IS adjacency status changes (An IS-IS address family change indicates that an address family is added or deleted.)	The **adjacency-protocol-change** keyword was added to the **snmp-agent trap enable isis** command.
OSPFv3: Configuring a description for an OSPFv3 process.	The **description** command was added.
OSPFv3: Enabling OSPFv3 isolation	The **isolate enable** command was added.
OSPFv3: Associating an OSPFv3 interface with a track entry to adjust the cost of the interface based on the track entry state	The **ospfv3 track adjust-cost** command was added.
OSPFv3: Shutting down an OSPFv3 process	The **shutdown process** command was added.
BGP: Support for BGP dedicated address family view	The following commands were added: • **address-family dedicated** • **display bgp group dedicated** • **display bgp peer dedicated** • **display bgp routing-table dedicated** • **display bgp update-group dedicated** • **refresh bgp dedicated** • **reset bgp dedicated** The following commands are supported in BGP dedicated address family view: • **peer allow-as-loop** • **peer enable** • **peer next-hop-local** • **peer reflect-client** • **reflect between-clients** • **reflector cluster-id**
BGP: Minimizing the priority of the routes advertised to BGP peers	The following commands were added: • **advertise lowest-priority on-peer-up duration** • **advertise lowest-priority on-startup duration**

Feature	Command changes
	• **reset bgp advertise lowest-priority**
BGP: Setting the local device IP as the next hop of each BGP ECMP route for load balancing	The **ecmp-nexthop-local** keyword was added to the **balance** command.
BGP: Retaining the next hop of each BGP ECMP route for load balancing	The **ecmp-nexthop-unchanged** keyword was added to the **balance** command.
BGP: Enabling BGP to use routes with different IGP metrics to the next hop for load balancing	The **balance igp-metric-ignore** command was added.
BGP: Configuring the time that BGP must wait for other protocols to complete GR or NSR after BGP completes GR or NSR	The **bgp update-delay wait-other-protocol** command was added.
BGP: Enabling the specified BMP server to monitor all peers in all BGP-VPN instances	The **bmp server monitor all-vpn-instance** command was added.
BGP: Enabling the specified BMP server to monitor all peers in the current instance	The **bmp server monitor current-instance** command was added.
BGP: Displaying information about BGP peers monitored by the specified BMP server for the specified BGP instance	The **display bgp bmp server monitor-peer** command was added.
BGP: Displaying BGP route information by route attribute	• The **as-path** and **cluster-list** keywords were added to the **display bgp link-state** command. • The **as-path**, **cluster-list**, **community**, **ext-community**, *community-number*&<1-32>, *aa:nn*&<1-32>, **internet**, **no-advertise**, **no-export**, **no-export-subconfed**, **rt** *route-target*, and **soo** *site-of-origin* parameters were added to the **display bgp routing-table ipv4 multicast** command. • The **as-path** and **cluster-list** keywords were added to the **display bgp routing-table ipv4 rtfilter** command. • The **as-path**, **cluster-list**, **community**, **ext-community**, *community-number*&<1-32>, *aa:nn*&<1-32>, **internet**, **no-advertise**, **no-export**, **no-export-subconfed**, **rt** *route-target*, and **soo** *site-of-origin* parameters were added to the **display bgp routing-table ipv4 unicast** command. • The **as-path**, **cluster-list**, **community**, **ext-community**, *community-number*&<1-32>, *aa:nn*&<1-32>, **internet**, **no-advertise**, **no-export**, **no-export-subconfed**, **rt** *route-target*, and **soo** *site-of-origin* parameters were added to the **display bgp routing-table ipv6 multicast** command. • The **as-path**, **cluster-list**, **community**,

Feature	Command changes
	ext-community, *community-number*&<1-32>, *aa:nn*&<1-32>, **internet**, **no-advertise**, **no-export**, **no-export-subconfed**, **rt** *route-target*, and **soo** *site-of-origin* parameters were added to the **display bgp routing-table ipv6 unicast** command.
BGP: Configuring BGP NSR	The following commands were added: • **display bgp non-stop-routing status** • **non-stop-routing**
BGP: Displaying BGP peer or peer group information	The **interface**, *link-local-address*, and *interface-type interface-number* parameters were added to the **display bgp peer** command.
BGP: Displaying the ORF prefix information received by a peer	The **interface**, *link-local-address*, and *interface-type interface-number* parameters were added to the **display bgp peer received prefix-list** command.
BGP: Manually soft-resetting BGP sessions	The **interface**, *link-local-address*, and *interface-type interface-number* parameters were added to the **refresh bgp** command.
BGP: Resetting BGP sessions for the specified address family	The **interface**, *link-local-address*, and *interface-type interface-number* parameters were added to the **reset bgp** command.
IP routing basics: Enabling maintenance probe (MTP)	The **maintenance-probe enable** command was added.
IP routing basics/static routing/IPv6 static routing: Displaying the time of the latest next hop update	The **Age** field was added to the command output of the following commands: • **display rib nib** • **display route-direct nib** • **display ipv6 rib nib** • **display ipv6 route-direct nib** • **display route-static nib** • **display ipv6 route-static nib**
IP routing basics: Specifying an alarm threshold, in percentage, on the number of active route prefixes	The *warn-threshold* argument was added to the **routing-table limit** command.
IPv6 static routing: Enabling periodic sending of ND requests to the next hops of IPv6 static routes	The **ipv6 route-static nd-request** command was added.
RIP: Configuring RIPv2 keychain authentication	The **keychain** keyword was added to the **rip authentication-mode** command.
Routing policy: Removing specific AS numbers or clearing the AS_PATH attribute	The **delete** and **clear** keywords were added to the **apply as-path** command.
Routing policy: Setting a cost type for IS-IS routes or modify the MED value for BGP routes	The following keywords were added to the **apply cost-type** command: • **inherit-link-cost**: Uses the IGP link cost as the MED value of BGP routes.

Feature	Command changes
	• **internal-inc-ibgp**: For IS-IS, this keyword sets the cost type a matching IS-IS route to IS-IS internal route. For BGP, this keyword sets the MED value for a matching BGP route to the IGP metric of the route's next hop. • **med-plus-igp**: Sets the sum of the original MED value and the IGP metric value of next hop as the MED value for a matching BGP route.
Routing policy: Setting a label index value	The **apply label-index** command was added.
Routing policy: Setting an SID value	The **apply label-value** command was added.
Routing policy: Specifying an index number for an extended community list entry	The **index** keyword was added to the **ip extcommunity-list** command.
BGP: Displaying information about BGP peer relationship down events	The **display bgp troubleshooting** command was added.
BGP: Enabling conversational remote host route learning	The **forwarding-conversational-learning** command was added.
BGP: Configuring peers that are created through interfaces	• **interface-peer additional-paths** • **interface-peer advertise additional-paths best** • **interface-peer advertise origin-as-validation** • **interface-peer advertise-community** • **interface-peer advertise-ext-community** • **interface-peer advertise-policy exist-policy** • **interface-peer advertise-policy non-exist-policy** • **interface-peer allow-as-loop** • **interface-peer as-number** • **interface-peer as-path-acl** • **interface-peer bfd** • **interface-peer bmp server** • **interface-peer capability-advertise orf prefix-list** • **interface-peer default-route-advertise** • **interface-peer description** • **interface-peer dscp** • **interface-peer enable** • **interface-peer fake-as** • **interface-peer filter-policy** • **interface-peer graceful-restart timer restart extra** • **interface-peer group** • **interface-peer ignore** • **interface-peer ignore-first-as** • **interface-peer ignore-originatorid**

Feature	Command changes
	• **interface-peer keep-all-routes** • **interface-peer keychain** • **interface-peer log-change** • **interface-peer low-memory-exempt** • **interface-peer next-hop-local** • **interface-peer nexthop-recursive-policy disable** • **interface-peer password** • **interface-peer preferred-value** • **interface-peer prefix-list** • **interface-peer public-as-only** • **interface-peer reflect-client** • **interface-peer route-limit** • **interface-peer route-policy** • **interface-peer route-update-interval** • **interface-peer soo** • **interface-peer substitute-as** • **interface-peer timer** • **interface-peer timer connect-retry**
BGP: Configuring BGP to advertise the BGP RPKI validation state to a peer or peer group	The **peer advertise origin-as-validation** command is supported in BGP VPNv4 address family view and BGP VPNv6 address family view.
BGP: Enabling BFD for the link to a BGP peer or peer group	The **echo** keyword was added to the **peer bfd** command.
BGP: Removing private AS numbers in BGP updates sent to an EBGP peer or peer group	The **force**, **limited**, **replace**, and **include-peer-as** keywords were added to the **peer public-as-only** command.
BGP: Configuring BGP maintenance features	The **shutdown process** command and the **isolate enable** command were added.
BGP: Specifying the longest match principle for BGP next hop recursion	The **nexthop recursive-lookup longest-match** command was added.
BGP: Configuring the BMP client to send peer down notifications with mode flags to the BMP server	The **pd-monitor-mode enable** command was added.
BGP: Configuring the BMP client to send peer up notifications with mode flags to the BMP server	The **pu-monitor-mode enable** command was added.
BGP: Enabling BGP to check the first AS number of EBGP routes (BGP will not advertise an EBGP route to EBGP peers whose AS number is the route's first AS number.)	The **peer-as-check enable** command was added.
BGP: Enabling BGP to send routes exchanged with the specified monitored peer or	The **peer route-mode** command was added.

Feature	Command changes
peer group to the BMP server.	
BGP: Associating a BGP peer or peer group with a track entry (BGP can adjust the priority of routes received from the peer or peer group based on the track entry state.)	The **peer route-priority-track** command was added.
BGP: Configuring the device as a route server and specifying a peer or peer group as a client	The **peer route-server-client** command was added.
BGP: Setting the TCP maximum segment size (MSS) for a peer or peer group	The **peer tcp-mss** command was added.
BGP: Enabling peer unreachability detection	The **peer tracking** command was added.
BGP: Using control-mode BFD to detect the connectivity to the next hop of the primary route	The **ctrl** keyword was added to the **primary-path-detect bfd** command.
BGP: Resetting the connection to a BMP server and clear statistics information	The **reset bgp bmp server** command was added.
BGP: Enabling BGP to send routes received from all the monitored peers and peer groups to the BMP server	The **route-mode adj-rib-in** command was added.
BGP: Configuring BGP to send routes advertised to the monitored peer or peer group to the BMP server	The **pre-policy**, **post-policy**, and **both** keywords were added to the **route-mode adj-rib-out** command.
BGP: Enabling BGP route advertisement delay	The **route-update-delay** command was added.
BGP: Configuring an IP address and port number for a BMP server	The *ipv6-address* argument was added to the **server** command.
BGP: Specifying the authentication mode and key for BGP to establish TCP connections to the BMP server	The **server password** command was added.
BGP: Specifying the source address of TCP connections to the BMP server	The **server source-address** command was added.
BGP: New BGP notification types	The following keywords were added to the **snmp-agent trap enable bgp** command: • **peer-addrfamily-routeexceed** • **peer-addrfamily-routeexceed-clear** • **peer-addrfamily-routethreshold-clear** • **peer-addrfamily-routethreshold-exceed** • **peer-backward-transition** • **peer-established** • **peer-routeexceed**

Feature	Command changes
	• **peer-routeexceed-clear** • **peer-routethreshold-clear** • **peer-routethreshold-exceed**
BGP: Enabling fast host route update upon user migration	The **user-move fast-update** command was added.
DCN features	All DCN commands were newly added.

New features: IP multicast features

Table 5 describes the IP multicast features added in this software version.

For more information about the features, see *IP Multicast Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *IP Multicast Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 5 IP multicast features added in Release 6710

Feature	Command changes
IGMP snooping/MLD snooping: Preventing the device from forwarding multicast data to router ports in a VLAN	The following commands were added: • **igmp-snooping router-port-discard** • **mld-snooping router-port-discard**
IGMP snooping/MLD snooping: Enabling the device to send IGMP/MLD general queries upon a port state change	The following commands were added: • **igmp-snooping triggered-query enable** • **mld-snooping triggered-query enable**
IGMP snooping/MLD snooping: Configuring a multicast access control policy	The following commands were added: • **igmp-snooping access-policy** • **mld-snooping access-policy**
Multicast routing and forwarding: Setting the maximum number of copied multicast packets during software forwarding	The **multicast cpu-forwarding max-copy-count** command was added.
Multicast routing and forwarding/IPv6 multicast routing and forwarding: Configuring multicast load splitting	The following parameters were added to the **load-splitting** (IPv6 MRIB view) and **load-splitting** (MRIB view) commands: • **balance-ecmp** • **balance-ucmp** • **ecmp** • **ucmp**
IGMP: Specifying an ACL by its name when configuring a filtering rule in IGMP	The **name** *ipv4-acl-name* option was added to the **igmp group-policy** and **ssm-mapping** commands.
PIM: Specifying an ACL by its name when configuring a filtering rule in PIM	The **name** *ipv4-acl-name* option was added to the following commands:

Feature	Command changes
	• **c-rp** • **pim neighbor-policy** • **register-policy** • **source-policy** • **ssm-policy** • **static-rp**
PIM/IPv6 PIM: Setting the timer for C-BSRs to wait BSMs from the BSR	The following commands were added: • **c-bsr holdtime** (PIM view) • **c-bsr holdtime** (IPv6 PIM view)
PIM/IPv6 PIM: Setting the interval for C-BSRs to send BSMs	The following commands were added: • **c-bsr interval** (PIM view) • **c-bsr interval** (IPv6 PIM view)
PIM/IPv6 PIM: Setting the delay timer for DR election	The following commands were added: • **pim timer dr-elect-delay** • **ipv6 pim timer dr-elect-delay**
PIM/IPv6 PIM: Enabling the device to send hello messages with a different Generation ID upon a port state change	The following commands were added: • **pim triggered-hello enable** • **ipv6 pim triggered-hello enable**
PIM/IPv6 PIM: Setting the interval for C-BSRs to send BSMs	The following commands were added: • **c-bsr interval** (PIM view) • **c-bsr interval** (IPv6 PIM view)
PIM/IPv6 PIM: Configuring a PIM/IPv6 PIM join policy to filter joined multicast sources and groups in PIM join or prune messages on an interface	The following commands were added: • **pim join-policy** • **ipv6 pim join-policy**
PIM/IPv6 PIM: Configuring an interface as a DR interface	The following commands were added: • **pim distributed-dr** • **ipv6 pim distributed-dr**
PIM/IPv6 PIM: Enabling SNMP notifications	The **interface-election** and **rp-mapping-change** parameters were added to the following commands: • **snmp-agent trap enable pim** • **snmp-agent trap enable pim6**
Multicast VPN: Displaying BGP MDT routing information	The **as-path** and **cluster-list** parameters were added to the **display bgp routing-table ipv4 mdt** command.
Multicast VPN: Displaying BGP IPv4 MVPN routing information	The following parameters were added to the **display bgp routing-table ipv4 mvpn** command: • **as-path** • **cluster-list** • **ext-community** • **rt** *route-target* • **whole-match**
IPv6 multicast routing and forwarding: Deleting all	The **delete ipv6 rpf-route-static**

Feature	Command changes
static IPv6 multicast routes	command was added.
IPv6 multicast routing and forwarding: Displaying static IPv6 multicast routing entries	The **display ipv6 multicast routing-table static** command was added.
IPv6 multicast routing and forwarding: Configuring a static IPv6 multicast route	The **ipv6 rpf-route-static** command was added.
IPv6 multicast routing and forwarding: Setting the maximum number of copied multicast packets during software forwarding	The **ipv6 multicast cpu-forwarding max-copy-count** command was added.
MLD: Specifying an IPv6 ACL by its name when configuring an IPv6 multicast group policy or MLD SSM mapping	The **name** *ipv6-acl-name* option was added to the **mld group-policy** and **ssm-mapping** commands.
IPv6 PIM: Specifying an IPv6 ACL by its name when configuring a filtering rule in IPv6 PIM	The **name** *ipv6-acl-name* option was added to the following commands: • **static-rp** • **c-rp** • **register-policy** • **ssm-policy** • **source-policy** • **ipv6 pim neighbor-policy**
IPv6 PIM: Displaying information about the IPv6 PIM routing entries for MVPN extranet	The **extranet** parameter was added to the **display ipv6 pim routing-table** command.

New features: ACL and QoS features

Table 6 describes the ACL and QoS features added in this software version.

For more information about the features, see *ACL and QoS Configuration Guide* in in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *ACL and QoS Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 6 ACL and QoS features in Release 6710

Feature	Command changes
ACL: Matching object groups in an ACL rule	The **object-group** *port-group-name* option was added to the following commands: • **rule** (IPv4 advanced ACL view) • **rule** (IPv4 basic ACL view) • **rule** (IPv6 advanced ACL view) • **rule** (IPv6 basic ACL view)
ACL: Matching inner TCP flags of VXLAN packets in an advanced ACL rule	The following option was added to the **rule** (IPv4 advanced ACL view) and **rule** (IPv6 advanced ACL view) commands: { **inner-ack** *inner-ack-value* | **inner-fin** *inner-fin-value* | **inner-psh** *inner-psh-value* | **inner-rst**

Feature	Command changes
	inner-rst-value | **inner-syn** *inner-syn-value* | **inner-urg** *inner-urg-value* } *
ACL: Matching the inner IP precedence in an IPv4 advanced ACL rule	The **inner-precedence** *inner-precedence* option was added to the **rule** (IPv4 advanced ACL view) command.
ACL: Matching the inner ToS in an IPv4 advanced ACL rule	The **inner-tos** *inner-tos* option was added to the **rule** (IPv4 advanced ACL view) command.
ACL: Matching the inner ECN flag in an IPv4 advanced ACL rule	The **inner-ecn** *inner-ecn* option was added to the **rule** (IPv4 advanced ACL view) command.
ACL: Matching the inner DSCP value in an IPv4 advanced ACL rule	The **inner-dscp** *inner-dscp* option was added to the **rule** (IPv4 advanced ACL view) command.
ACL: ACL: Matching the inner header information of VXLAN packets in an IPv6 advanced ACL rule	The following command was added: **rule** [*rule-id*] { **deny** | **permit** } **vxlan** [**vxlan-id** *vxlan-id*] **inner-protocol** *inner-protocol* [**counting** | **inner-destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **inner-destination-port** *operator port1* [*port2*] | { { **inner-ack** *inner-ack-value* | **inner-fin** *inner-fin-value* | **inner-psh** *inner-psh-value* | **inner-rst** *inner-rst-value* | **inner-syn** *inner-syn-value* | **inner-urg** *inner-urg-value* } * | **inner-established** } | **inner-source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **inner-source-port** *operator port1* [*port2*] | { **inner-dscp** *inner-dscp* | **inner-ecn** *inner-ecn* } * | **logging** | **time-range** *time-range-name*] *
QoS: Mirroring-type QoS policy	The **mirroring** keyword was added to the following commands: • **display qos policy interface** • **display qos policy global** • **display qos policy user-defined** • **display qos policy l2vpn-ac** • **display qos policy diagnosis global** • **display qos policy diagnosis interface** • **qos apply policy** (Ethernet service instance view, interface view, control plane view) • **qos apply policy global** • **qos policy** • **reset qos policy global**

Feature	Command changes
QoS: Clearing the QoS policies applied to Ethernet service instances	The **reset qos policy l2vpn-ac** command was added.

New features: Security features

Table 7 describes the security features added in this software version.

For more information about the features, see *Security Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Security Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 7 Security features added in Release 6710

Feature	Command changes
AAA: Configuring the authentication failure policy for users in an ISP domain	The **authen-fail** command was added.
AAA: Specifying an action to take on users in the critical domain when a RADIUS server becomes available	The **authen-radius-recover** command was added.
AAA: Specifying a critical domain to accommodate users that access the ISP domain when all RADIUS servers are unavailable	The **authen-radius-unavailable online domain** command was added.
AAA: Configuring authorization attributes for users in an ISP domain	The **vlan** and **vsi** keywords were added to the **authorization-attribute** command.
AAA: Enabling temporary redirect	The **redirect move-temporarily enable** command was added.
AAA: Configuring authorization attributes for a network access user or user group	The **url** keyword was added to the **authorization-attribute** command.
AAA: Configuring local guests	The **guest** keyword was added to the **local-user** and **display local-user** commands. The following commands were added: • **company** • **display local-guest waiting-approval** • **email** • **full-name** • **local-guest email format** • **local-guest email sender** • **local-guest email smtp-server** • **local-guest generate** • **local-guest manager-email** • **local-guest send-email** • **local-guest timer** • **phone** • **reset local-guest waiting-approval**

Feature	Command changes
	• **sponsor-department** • **sponsor-email** • **sponsor-full-name** • **validity-datetime**
AAA: Exporting local guest account information to a .csv file in the specified path	The **local-user-export** command was added.
AAA: Importing local guest account information from a .csv file in the specified path to the device to create local guests based on the imported information	The **local-user-import** command was added.
AAA: Configuring the format of the RADIUS NAS-Port attribute	The **attribute 5 format** command was added.
AAA: Configuring the MAC address format for the RADIUS Called-Station-Id attribute	The **attribute 30 mac-format** command was added.
AAA: Configuring the MAC address format for the RADIUS Calling-Station-Id attribute	The **one** keyword was added to the **attribute 31 mac-format** command.
AAA: Configuring the format of RADIUS attribute 87	The **attribute 87 format** command was added.
AAA: Including subattribute 218 of vendor 25506 in outgoing RADIUS packets	The **include-attribute 218 vendor-id 25506** command was added.
AAA: Specifying a source IP address for outgoing RADIUS packets	The **nas-ip** command was added.
AAA: Configuring the device to preferentially process RADIUS authentication requests	The **radius authentication-request first** command was added.
AAA: Setting the interval at which the device detects the status of RADIUS authentication servers	The **radius-server authen-state-check interval** command was added.
AAA: Displaying HWTACACS packet statistics	The **display hwtacacs statistics** command was added.
AAA: Setting the DSCP priority for RADIUS packets	The **hwtacacs dscp** command was added.
802.1X: Displaying online 802.1X user information	The **m-lag** [**local** | **peer**] and **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** } parameters were added to the **display dot1x connection** command.
802.1X: Displaying unknown source MAC addresses in the unicast-trigger quiet period	The **display dot1x unicast-trigger quiet-mac** command was added.
802.1X: Enabling generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users	The **dot1x** { **ip-verify-source** | **ipv6-verify-source** } **enable** command was added.
802.1X: Configuring 802.1X	The following commands were added to Layer 2 aggregate interface view: • **dot1x after-mac-auth max-attempt** • **dot1x auth-fail eapol** • **dot1x auth-fail vlan**

Feature	Command changes
	• **dot1x critical eapol** • **dot1x critical vlan** • **dot1x critical-voice-vlan** • **dot1x eap-tls-fragment to-server** • **dot1x eapol untag** • **dot1x guest-vlan** • **dot1x guest-vlan-delay** • **dot1x guest-vsi-delay** • **dot1x handshake** • **dot1x handshake reply enable** • **dot1x handshake secure** • **dot1x mac-binding** • **dot1x mac-binding enable** • **dot1x mandatory-domain** • **dot1x multicast-trigger** • **dot1x offline-detect enable** • **dot1x port-control** • **dot1x port-method** • **dot1x re-authenticate** • **dot1x re-authenticate manual** • **dot1x re-authenticate server-unreachable keep-online** • **dot1x server-recovery online-user-sync** • **dot1x timer reauth-period** • **dot1x unauthenticated-user aging enable** • **dot1x unicast-trigger** • **dot1x user-ip freeze**
802.1X: Enabling online 802.1X users to escape from offline detection and stay online when no reachable RADIUS authentication servers are available	The **dot1x auth-server-unavailable escape** command was added.
802.1X: Discarding duplicate 802.1X EAPOL-Start requests	The **dot1x duplicate-eapol-start discard** command was added.
802.1X: Configuring the redirect URL if users will use Web browsers to access the network	The **secondary** and **track** *track-entry-number* parameters were added to the **dot1x ead-assistant url** command.
802.1X: Setting the maximum number of concurrent 802.1X users on a port	The **preauth-domain** and **auth-fail-domain** keywords were added to the **dot1x max-user** command.
802.1X: Setting an 802.1X timer	The **unicast-trigger quiet-period** *quiet-period-value* option was added to the **dot1x timer** command.
802.1X: Logging off 802.1X users	The **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** |

Feature	Command changes
	success } parameters were added to the **reset dot1x access-user** command.
802.1X: Removing the records of unknown source MAC addresses in the unicast-trigger quiet period	The **reset dot1x unicast-trigger quiet-mac** command was added.
MAC authentication: Displaying information about online MAC authentication users	The **m-lag** [**local** | **peer**] and **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } parameters were added to the **display mac-authentication connection** command.
MAC authentication: Displaying MAC authentication user recovery profiles	The **display mac-authentication user-recovery-profile** command was added.
MAC authentication: Configuring the username and password for accessing the RESTful server	The **login-name** command was added.
MAC authentication: Enabling online MAC authentication users to escape from offline detection and stay online when no reachable RADIUS authentication servers are available	The **mac-authentication auth-server-unavailable escape** command was added.
MAC authentication: Enabling automatic MAC authentication user recovery	The **mac-authentication auto-recover-user** command was added.
MAC authentication: Configuring MAC authentication	The following commands were added to Layer 2 aggregate interface view: • **mac-authentication critical vlan** • **mac-authentication critical-voice-vlan** • **mac-authentication domain** • **mac-authentication guest-vlan** • **mac-authentication guest-vlan auth-period** • **mac-authentication offline-detect enable** • **mac-authentication parallel-with-dot1x** • **mac-authentication re-authenticate** • **mac-authentication re-authenticate server-unreachable keep-online** • **mac-authentication server-recovery online-user-sync** • **mac-authentication timer** • **mac-authentication unauthenticated-user aging enable**
MAC authentication: Specifying the MAC authentication critical VLAN on the port	The **url-user-logoff** keyword was added to the **mac-authentication critical vlan**

Feature	Command changes
	command.
MAC authentication: Enabling guest VLAN reauthentication in MAC authentication	The **mac-authentication guest-vlan re-authenticate** command was added.
MAC authentication: Enabling guest VSI reauthentication in MAC authentication	The **mac-authentication guest-vsi re-authenticate** command was added.
MAC authentication: Configuring a username and password for MAC authentication users in a MAC address range	The **mac-authentication mac-range-account** command was added.
MAC authentication: Setting the maximum number of concurrent MAC authentication users on a port	The **preauth-domain** and **auth-fail-domain** keywords were added to the **mac-authentication max-user** command.
MAC authentication: Manually recovering MAC authentication users	The **mac-authentication recover-user** command was added.
MAC authentication: Associating a redirect URL for MAC authentication users with a track entry	The **mac-authentication redirect-url** command was added.
MAC authentication: Configuring a MAC authentication timer	The **temporary-user-aging** *aging-time-value* option was added to the **mac-authentication timer** command.
MAC authentication: Configuring the global user account policy for all MAC authentication users	The **separator colon** keywords were added to the **mac-authentication user-name-format** command.
MAC authentication: Creating a profile for MAC authentication user recovery and enter its view	The **mac-authentication user-recovery-profile** command was added.
MAC authentication: Configuring Web proxy ports for URL redirection in MAC authentication	The **mac-authentication web-proxy** command was added.
MAC authentication: Configuring the NAS IP address used by the device to communicate with the RESTful server	The **nas-ip** command was added.
MAC authentication: Logging off MAC authentication users	The **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } parameters were added to the **reset mac-authentication access-user** command.
MAC authentication: Configuring the IP address and port number of the RESTful server	The **server-address** command was added.
Portal authentication: Setting the aging time for MAC-trigger entries	The **aging-time** command was added.
Portal authentication: Setting the timeout the device waits for portal authentication to complete after receiving the MAC binding query response	The **authentication-timeout** command was added.
Portal authentication: Setting the maximum number of attempts and the interval for sending MAC binding queries to the MAC binding server	The **binding-retry** command was added.
Portal authentication: Enabling cloud MAC-trigger authentication	The **cloud-binding enable** command was added.

Feature	Command changes
Portal authentication: Specifying the URL of the cloud portal authentication server	The **cloud-server url** command was added.
Portal authentication: Displaying information about MAC binding servers	The **display portal mac-trigger-server** command was added.
Portal authentication: Displaying packet statistics for portal authentication servers	The **extend-auth-server cloud** keywords were added to the **display portal packet statistics** command.
Portal authentication: Displaying session information for portal users or portal-based Web authentication users	The **display portal session user-type** command was added.
Portal authentication: Displaying portal user information	The following parameters were added to the **display portal user** command: • **auth-type** { **cloud** | **local** | **normal** } • **mac** *mac-address* • **username** *username* • **brief**
Portal authentication: Setting the free-traffic threshold	The **free-traffic threshold** command was added.
Portal authentication: Specifying the IPv4 address of a MAC binding server	The **ip** (MAC binding server view) command was added.
Portal authentication: Specifying the IPv6 address of a MAC binding server	The **ipv6** (MAC binding server view) command was added.
Portal authentication: Binding an SSID or endpoint name to an authentication page file	The **logon-page bind** command was added.
Portal authentication: Configuring the NAS-Port-Type attribute carried in outgoing RADIUS requests on the interface	The **nas-port-type** command was added.
Portal authentication: Setting the maximum number of portal users allowed on an interface	The **max-user** keyword was added to the **portal** { **ipv4-max-user** | **ipv6-max-user** | **max-user** } command.
Portal authentication: Obtaining user access information from ARP or ND entries	The **portal access-info trust** command was added.
Portal authentication: Specifying a MAC binding server on an interface	The **portal** [**ipv6**] **apply mac-trigger-server** command was added.
Portal authentication: Specifying a portal Web server for redirect of HTTP requests sent by unauthenticated portal users	The **secondary** keyword was added to the **portal apply web-server** command.
Portal authentication: Logging out online portal users	The **auth-type** { **cloud** | **local** | **normal** } and **mac** *mac-address* parameters were added to the **portal delete-user** command.
Portal authentication: Setting the authentication load sharing mode for portal users on M-LAG interfaces	The **portal m-lag load-sharing-mode** command was added.
Portal authentication: Setting the traffic backup interval and threshold for portal users on M-LAG interfaces	The **portal m-lag traffic backup** command was added.

Feature	Command changes
Portal authentication: Enabling the portal fail-permit feature for portal Web servers	The **portal fail-permit web-server** command was added.
Portal authentication: Setting the user synchronization interval for portal authentication using OAuth	The **portal oauth user-sync interval** command was added.
Portal authentication: Clearing packet statistics for portal authentication servers.	The **extend-auth-server cloud** keywords were added to the **reset portal packet statistics** command.
Portal authentication: Specifying the type of a MAC binding server	The **server-type** command was added.
Portal authentication: Configuring the parameters to be carried in the URL when the device redirects it to users	The **format section** { **1** | **3** | **6** } { **lowercase** | **uppercase** } keywords were added to the **url-parameter** command.
Portal authentication: Specifying the version of the portal protocol	The **version** command was added.
Web authentication: Displaying Web authentication user information	The **m-lag** [**local** | **peer**] keywords were added to the **display web-auth user** command.
Web authentication: Logging off Web authentication users	The **reset web-auth access-user** command was added.
Web authentication: Configuring the redirection URL of the Web server for Web authentication	The **track** *track-entry-number* option was added to the **url** command.
Web authentication: Configuring the unescaped special characters in the Web authentication URL redirected to users	The **url-unescape-chars** command was added.
Web authentication: Applying a portal MAC binding server for Web authentication	The **web-auth apply portal mac-trigger-server** command was added.
Web authentication: Creating a remote Web server for Web authentication	The following commands were added: • **web-auth remote server** *server-name* • **ip** (Web authentication remote Web server view) • **ipv6** (Web authentication remote Web server view) • **url** • **url-parameter** • **url-unescape-chars**
Web authentication: Configuring Web authentication	The following commands were added to Layer 2 aggregate interface view: • **web-auth auth-fail vlan** • **web-auth domain** • **web-auth enable** • **web-auth offline-detect**
Web authentication: Enabling online detection bypass for Web authentication users	The **web-auth auth-server-unavailable escape** command was added.

Feature	Command changes
Web authentication: Enabling Web authentication	The **secondary-server** *secondary-server-name* option was added to the **web-auth enable** command.
Web authentication: Configuring a Web authentication-free host name	The **web-auth free-host** command was added.
Web authentication: Configuring Web authentication multi-VLAN mode	The **web-auth host-mode multi-vlan** command was added.
Web authentication: Setting the maximum number of Web authentication users	The **preauth-domain** and **auth-fail-domain** keywords were added to the **web-auth max-user** command.
Web authentication: Adding the port number of a Web proxy server	The **https** keyword was added to the **web-auth proxy port** command.
Web authentication: Configuring the aging timer for temporary MAC address entries	The **web-auth timer temp-entry-aging** command was added.
Port security: Displaying entries for online port security access users	The **display port-security access-user** command was added.
Port security: Displaying port security statistics	The **display port-security statistics** command was added.
Port security: Configuring port security	The following commands were added to Layer 2 aggregate interface view: • **port-security authentication open** • **port-security authorization ignore** • **port-security escape critical-vsi** • **port-security intrusion-mode** • **port-security mac-address aging-type inactivity** • **port-security mac-address dynamic** • **port-security mac-address security** • **port-security mac-limit** • **port-security max-mac-count** • **port-security nas-id-profile** • **port-security port-mode**
Port security: Configuring an authentication load sharing mode for users attached to M-LAG interfaces	The **port-security m-lag load-sharing-mode** command was added.
Port security: Enabling VLAN check bypass for users moving to the port from other ports	The **port-security mac-move bypass-vlan-check** command was added.
Port security: Enabling MAC move	The **port** and **vlan** keywords were added to the **port-security mac-move permit**

Feature	Command changes
	command.
Port security: Setting the port security mode of a port	The **mac-and-userlogin-secure-ext** keyword was added to the **port-security port-mode** command.
Port security: Specifying a preauthentication domain for port security users on a port	The **port-security pre-auth domain** command was added.
Port security: Configuring static users for port access authentication	The following commands were added: • **display port-security static-user** • **display port-security static-user connection** • **port-security static-user** • **port-security static-user match-mac acl** • **port-security static-user max-user** • **port-security static-user password** • **port-security static-user timer detect-period** • **port-security static-user timer offline-detect** • **port-security static-user update-ip enable** • **port-security static-user user-name-format** • **port-security static-user user-name-format mac-address** • **reset port-security static-user**
Port security: Setting port security timers	The **port-security timer** command was added.
Port security: Configuring the trigger order for authentication methods on the port as MAC authentication, 802.1X authentication, and Web authentication	The **port-security triple-auth-order mac-dot1x-web** command was added.
Port security: Specifying a domain for port security users redirected to an unavailable URL	The **port-security url-unavailable domain** command was added.
Port security: Clearing port security statistics.	The **reset port-security statistics** command was added.
Object group features	All Object group commands were newly added.
Attack detection and prevention: Clearing attack detection and prevention statistics for an interface	The **reset attack-defense statistics interface** *interface-type interface-number* command was added.
Attack detection and prevention: Displaying information about IPv4 scanning attackers	The **interface** *interface-type interface-number* option was added to the **display attack-defense scan attacker ip** command.

Feature	Command changes
Attack detection and prevention: Displaying information about IPv6 scanning attackers	The **interface** *interface-type interface-number* option was added to the **display attack-defense scan attacker ipv6** command.
Attack detection and prevention: Displaying information about IPv4 scanning attack victims	The **interface** *interface-type interface-number* option was added to the **display attack-defense scan victim ip** command.
Attack detection and prevention: Displaying information about IPv6 scanning attack victims	The **interface** *interface-type interface-number* option was added to the **display attack-defense scan victim ipv6** command.
ND attack defense: Ignoring ingress ports of ND packets in ND attack detection	The **ipv6 nd detection port-match-ignore** command was added.
ND attack defense: Displaying ND keepalive entries	The **display ipv6 nd scan keepalive entry** [**interface** *interface-type interface-number*] [**count**] command was added.
ND attack defense: Displaying statistics about NS packets sent to the IPv6 addresses in offline keepalive entries	The **display ipv6 nd scan keepalive statistics** [**slot** *slot-number*] [**interface** *interface-type interface-number*] command was added.
ND attack defense: Setting the aging time for ND keepalive entries	The **ipv6 nd scan keepalive aging-time** *time* command was added.
ND attack defense: Enabling the ND keepalive entry scanning feature	The **ipv6 nd scan keepalive enable** command was added.
ND attack defense: Setting the NS packet sending rate for keepalive entry scanning	The **ipv6 nd scan keepalive send-rate** *pps* command was added.
ND attack defense: Clearing statistics about NS packets sent to the IPv6 addresses in offline keepalive entries	The **reset ipv6 nd scan keepalive statistics** [**slot** *slot-number*] command was added.
ND attack defense: Enabling SNMP notifications for ND	The **snmp-agent trap enable nd** [**entry-limit** | **local-conflict** | **nd-miss** | **rate-limit**] * command was added.
Password control: Setting the maximum number of blacklist entries for a user account	The **password-control per-user blacklist-limit** command was added.
PKI: Enabling local certificate expiration notification	The **pki certificate logging enable** command was added.
SSH: Displaying records for SSH user login exceptions	The **display ssh exception-record** command was added.
SSH: Setting the maximum number of records for SSH user login exceptions	The **ssh exception-record max-number** command was added.
SSH: Setting alarm and recovery thresholds for SSH user login failures in the specified statistics period	The **ssh server login-failed threshold-alarm** command was added.

Feature	Command changes
IP source guard: Displaying local IPv4SG bindings that can be synchronized by routing protocols	The **display ip source binding-local** command was added.
IP source guard: Displaying remote IPv4SG bindings synchronized by routing protocols	The **display ip source binding-remote** command was added.
IP source guard: Displaying statistics about local and remote IPv4SG bindings that routing protocols synchronize	The **display ip source binding statistics** command was added.
IP source guard: Displaying local IPv6SG bindings that can be synchronized by routing protocols	The **display ipv6 source binding-local** command was added.
IP source guard: Displaying remote IPv6SG bindings synchronized by routing protocols	The **display ipv6 source binding-remote** command was added.
IP source guard: Displaying statistics about local and remote IPv6SG bindings that routing protocols synchronize	The **display ipv6 source binding statistics** command was added.
ARP attack protection: Displaying ARP source suppression entries	The **display arp source-suppression cache** command was added.
ARP attack protection: Setting the ARP packet sending rate for automatic ARP scanning	The **arp scan auto send-rate** command was added.
ARP attack protection: Enabling automatic ARP scanning	The **arp scan auto enable** command was added.
ARP attack protection: Setting the ARP request sending rate for keepalive entry scanning	The **arp scan keepalive send-rate** command was added.
ARP attack protection: Setting the aging time for ARP keepalive entries	The **arp scan keepalive aging-time** command was added.
ARP attack protection: Enabling the ARP keepalive entry scanning feature	The **arp scan keepalive enable** command was added.
ARP attack protection: Displaying ARP keepalive entries	The **display arp scan keepalive entry** command was added.
ARP attack protection: Displaying statistics about ARP requests sent to the IP addresses in offline keepalive entries for an interface	The **display arp scan keepalive statistics** command was added.
ARP attack protection: Clearing statistics about ARP requests sent to the IP addresses in offline keepalive entries	The **reset arp scan keepalive statistics** command was added.
ARP attack protection: Enabling ARP gateway protection for a gateway	The **arp filter source** command was added.
ARP attack protection: Enabling SNMP notifications for ARP	The **snmp-agent trap enable arp** command was added.
IP source guard: Enabling IPv6SG	The **ipv6 verify source** command was added to VLAN view.
IP source guard: Displaying IPv4SG bindings	The **remote** keyword was added to the **display ip source binding** command.
ARP attack protection: Configuring a user validity check rule	The **vsi** *vsi-name* option was added to the **arp detection rule** command.
ARP attack protection: Enabling ARP attack detection logging	The **threshold** *threshold-value* option was

Feature	Command changes
	added to the **arp detection log enable** command.

New features: High availability features

Table 8 describes the high availability features added in this software version.

For more information about the features, see *High Availability Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *High Availability Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 8 High availability features added in Release 6710

Feature	Command changes
VRRP: Enabling the isolation mode for IPv4 VRRP	The **vrrp isolate enable** command was newly added.
VRRP: Setting the delay time for the IPv4 VRRP group to transition from **Initialize** to **Master** or **Backup** state	The **vrrp state-transition-delay** command was newly added.
VRRP: Enabling the isolation mode for IPv6 VRRP	The **vrrp ipv6 isolate enable** command was newly added.
VRRP: Setting the delay time for the IPv6 VRRP group to transition from **Initialize** to **Master** or **Backup** state	The **vrrp ipv6 state-transition-delay** command was newly added.
BFD: Setting the delay timer for BFD to notify upper-layer protocols of session establishment failures	The **bfd init-fail-timer** command was newly added.
BFD: Setting the minimum interval for receiving multihop BFD echo packets	The **bfd multi-hop min-echo-receive-interval** command was newly added.
BFD: Creating a static BFD session and entering its view, or entering the view of an existing static BFD session	The **bfd static** command was newly added.
BFD: Specifying the TTL value for BFD packets	The **bfd ttl** command was newly added.
BFD: Specifying the local and remote discriminators for a static BFD session	The **discriminator** command was newly added.
BFD: Displaying the TTL values for BFD packets	The **display bfd ttl** command was newly added.
Track: Creating a track entry associated with a static BFD session and entering track entry view, or entering the view of an existing track entry	The **track bfd static** command was newly added.
Track: Creating a track entry associated with M-LAG MAD state and entering track entry view, or entering the view of an existing track entry	The **track mlag-mad-status** command was newly added.
Track: Disabling checking whether the echo response receiving interface is consistent with the echo packet output interface	The **ignore-rx-interface** keyword was added to the **track bfd echo** command.

New features: Network management and monitoring features

Table 9 describes the network management and monitoring features added in this software version.

For more information about the features, see *Network Management and Monitoring Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Network Management and Monitoring Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 9 Network management and monitoring features added in Release 6710

Feature	Command changes
NTP: Disallowing control queries from peer devices to the local device	The **ntp-service noquery enable** command was added.
PTP: Displaying brief information about the PTP synchronization path from the GM to the device	The **display ptp path-trace** command was added.
PTP: Displaying historical role change information for PTP ports	The **display ptp port-history** command was added.
PTP: Enable PTP globally	The **ptp global enable** command was added.
PTP: Disabling PTP path tracing	The **ptp path-trace disable** command was added.
sFlow: Configuring sFlow collector information	The **dscp** *dscp-value* option was added to the **sflow collector** command.
Performance management	All performance management commands were newly added.
System maintenance and debugging: Tracing the path that the packets traverse from source to destination	The **-e** keyword was added to the following commands: • **tracert** • **tracert ipv6**
SNMP: Configuring the target host to which SNMP notifications are sent	The **cipher-securityname** *cipher-security-string* option was added to the **snmp-agent target-host** command.
SNMP: Specifying the notification format	The **snmp-agent trap format** command was added.
SNMP: Adding the device serial number (SN) to SNMP notifications sent from the device to the NMS	The **snmp-agent trap withsn** command was added.
EAA: Configuring an automatic email sending action	The following commands were added: • **rtm email domain** • **rtm email max-size** • **rtm email username password** • **action email**
EAA: Configuring a periodic event	The **event period** command was added.
Process monitoring and maintenance: Displaying free memory block information for a user process	The **display process memory fragment free** command was added.

Feature	Command changes
Process monitoring and maintenance: Displaying used memory block information for a user process	The **display process memory fragment used** command was added.
Information center: Setting the format for logs sent to log hosts	The **rfc5424** keyword was added to the **info-center format** command.
Information center: Adding the device serial number to the location field of logs sent to log hosts	The **info-center loghost locate-info with-sn** command was added.
VCF fabric: Specifying the NETCONF username and password for automated VCF fabric deployment	The following commands were added: • **vcf-fabric underlay netconf-username** • **vcf-fabric underlay netconf-password**
NETCONF: Displaying current NETCONF service status and global NETCONF service statistics	The **display netconf service** command was added.
NETCONF: Displaying NETCONF session status and statistics	The **display netconf session** command was added.
NETCONF: Clearing current global NETCONF service statistics	The **reset netconf service statistics** command was added.
NETCONF: Clearing current NETCONF session statistics	The **reset netconf session statistics** command was added.
NETCONF: Enabling conversion of NETCONF operations to logs and commands	The **netconf log xml2cli enable** command was added.
OpenFlow: Specifying a controller for an OpenFlow switch and configuring the main connection to the controller	The **global-ssl** keyword was added to the **controller address** command.
Feature	**Command changes**
NTP: Disallowing control queries from peer devices to the local device	The **ntp-service noquery enable** command was added.
PTP: Displaying brief information about the PTP synchronization path from the GM to the device	The **display ptp path-trace** command was added.
PTP: Displaying historical role change information for PTP ports	The **display ptp port-history** command was added.
PTP: Enable PTP globally	The **ptp global enable** command was added.
PTP: Disabling PTP path tracing	The **ptp path-trace disable** command was added.
sFlow: Configuring sFlow collector information	The **dscp** *dscp-value* option was added to the **sflow collector** command.
Performance management	All performance management commands were newly added.
System maintenance and debugging: Tracing the path that the packets traverse from source to destination	The **-e** keyword was added to the following commands: • **tracert** • **tracert ipv6**

Feature	Command changes
SNMP: Configuring the target host to which SNMP notifications are sent	The **cipher-securityname** *cipher-security-string* option was added to the **snmp-agent target-host** command.
SNMP: Specifying the notification format	The **snmp-agent trap format** command was added.
SNMP: Adding the device serial number (SN) to SNMP notifications sent from the device to the NMS	The **snmp-agent trap withsn** command was added.
EAA: Configuring an automatic email sending action	The following commands were added: • **rtm email domain** • **rtm email max-size** • **rtm email username password** • **action email**
EAA: Configuring a periodic event	The **event period** command was added.
Process monitoring and maintenance: Displaying free memory block information for a user process	The **display process memory fragment free** command was added.
Process monitoring and maintenance: Displaying used memory block information for a user process	The **display process memory fragment used** command was added.
Information center: Setting the format for logs sent to log hosts	The **rfc5424** keyword was added to the **info-center format** command.
Information center: Adding the device serial number to the location field of logs sent to log hosts	The **info-center loghost locate-info with-sn** command was added.
VCF fabric: Specifying the NETCONF username and password for automated VCF fabric deployment	The following commands were added: • **vcf-fabric underlay netconf-username** • **vcf-fabric underlay netconf-password**
NETCONF: Displaying current NETCONF service status and global NETCONF service statistics	The **display netconf service** command was added.
NETCONF: Displaying NETCONF session status and statistics	The **display netconf session** command was added.
NETCONF: Clearing current global NETCONF service statistics	The **reset netconf service statistics** command was added.
NETCONF: Clearing current NETCONF session statistics	The **reset netconf session statistics** command was added.
NETCONF: Enabling conversion of NETCONF operations to logs and commands	The **netconf log xml2cli enable** command was added.

New features: Telemetry features

Table 10 describes the telemetry features added in this software version.

For more information about the features, see *Telemetry Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Telemetry Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 10 Telemetry features added in Release 6710

Feature	Command changes
gRPC: Displaying detailed gRPC information	The **verbose** keyword was added to the **display grpc** command.
gRPC: Setting the maximum CPU usage for gRPC	The **grpc cpu-usage max-percent** command was added.
gRPC: Displaying sensor paths that have the minimum sampling interval	The **display telemetry sensor-path** command was added.
gRPC: Adding an IPv4 collector to the destination group by its domain name	The **domain-name** command was added.
gRPC: Adding an IPv6 collector to the destination group by its domain name	The **ipv6 domain-name** command was added.
gRPC: Setting the DSCP value for packets sent to collectors	The **dscp** command was added.
gRPC: Enabling TLS to encrypt the gRPC connection between the device and the specified IPv4 collector	The **tls** keyword was added to the **ipv4-address** command.
gRPC: Enabling TLS to encrypt the gRPC connection between the device and the specified collector	The **tls** keyword was added to the **ipv6-address** command.
gRPC: Enabling per-row time-stamping for JSON-encoded subscription data	The **json row-timestamp enable** command was added.
gRPC: Setting the data push mode for a subscription	The **push-mode** command was added.
gRPC: Pushing data from specified nodes in a sensor path	The **selection-nodes** *node-list* option was added to the **sensor path** command.
gRPC: Specifying that the sensor group collects and pushes data at intervals in milliseconds	The **msec** keyword was added to the **sensor-group** command.
gRPC: Setting the data push suppression interval for a sensor group	The **suppress-time** *suppress-time* option was added to the **sensor-group** command.
gRPC: Creating a gNMI sensor group	The **gnmi** keyword was added to the **sensor-group** command.
gRPC: Creating a gNMI subscription	The **gnmi** keyword was added to the **subscription** command.

New features: OpenFlow features

Table 11 describes the OpenFlow features added in this software version.

For more information about the features, see *OpenFlow Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *OpenFlow Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 11 OpenFlow features added in Release 6710

Feature	Command changes
Enabling SNMP notifications for OpenFlow	The **snmp-agent trap enable openflow** command was added.
Excluding the specified VLANs from the VLANs in which traffic is forwarded in the OpenFlow forwarding process	The **openflow normal-forward vlan** command was added.
OpenFlow: Specifying a controller for an OpenFlow switch and configuring the main connection to the controller	The **global-ssl** keyword was added to the **controller address** command.

New features: VXLAN features

Table 12 describes the VXLAN features added in Release 6710.

For more information about the features, see *VXLAN Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *VXLAN Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 12 VXLAN features added in Release 6710

Feature	Command changes
Disabling flooding the ARP requests that do not match any ARP flood suppression entries	The **no-broadcast** keyword was added to the **arp suppression enable** command.
Setting the ARP flood suppression mode	The **arp suppression mode** command was added.
Displaying information about the multicast groups that contain IGMP host-enabled interfaces for a VPN instance	The **vpn-instance** *vpn-instance-name* option was added to the **display igmp host group** command.
Displaying information about VXLAN tunnel interfaces	The **display vxlan tunnel-interface** command was added.
Disabling flooding the ND requests that do not match any ND flood suppression entries	The **no-broadcast** keyword was added to the **ipv6 nd suppression enable** command.
Setting the ND flood suppression mode	The **ipv6 nd suppression mode** command was added.

New features: Intelligent lossless network features

As from this release, documents about the PFC module move to document set Intelligent Lossless Network.

Table 13 describes the PFC features added in this software version.

For more information about the features, see *Intelligent Lossless Network Configuration Guide* in *HPE 5710 Switch Series Configuration Guides-Release 671x*.

For more information about the commands, see *Intelligent Lossless Network Command Reference* in *HPE 5710 Switch Series Command References-Release 671x*.

Table 13 PFC features added in Release 6710

Feature	Command changes
PFC: Configuring the action to take on an interface when the number of PFC deadlock times within the specified detection period exceeds the upper threshold	• The **priority-flow-control deadlock threshold action** command was added. • The **error-down** keyword was added to the **priority-flow-control deadlock threshold** command.

New features: M-LAG support for DRNI commands

The M-LAG feature was named DRNI in earlier software versions. For compatibility with earlier software versions, the device supports both M-LAG and DRNI commands.

Table 14 Difference between M-LAG and DRNI commands

Feature name	Keywords	Example
M-LAG	**m-lag**, **mlag**, **peer-link**	**m-lag system-number** *system-number* As a best practice, use M-LAG commands.
DRNI	**drni**, **drmac**, **ipp**	**drni system-number** *system-number* To use configuration files created from an earlier software version, use DRNI commands. The system recognizes only the complete syntaxes of DRNI commands. It does not support displaying available keywords and arguments in response to a question mark (?) or automatically completing the last keyword or argument in response to the Tab key. If you execute a DRNI command, the system converts it into the corresponding M-LAG command and saves the M-LAG command in the configuration file.

M-LAG and DRNI commands do not differ in the configuration method or functionality. For more information about the keyword differences, see comparison between M-LAG and DRNI commands see Modified feature: DRNI term changes.

New feature: FEC mode

Configuring FEC

About this task

The forward error correction (FEC) feature corrects packet errors to improve transmission quality. It attaches correction information to a packet at the sending end, and corrects error codes generated during transmission at the receiving end based on the correction information. You can set the FEC mode as needed.

Restrictions and guidelines

Make sure you set the same FEC mode for both interfaces of a link.

Procedure

1. Enter system view.
   `system-view`
2. Enter Ethernet interface view.
   `interface` *`interface-type interface-number`*
3. Set the FEC mode of the Ethernet interface.
   `port fec mode { auto | none | rs-fec }`
   By default, the FEC mode of an Ethernet interface is autonegotiated.

Command reference

port fec mode

Use **`port fec mode`** to set the forward error correction (FEC) mode of an interface.

Use **`undo port fec mode`** to restore the default.

Syntax

`port fec mode { auto | none | rs-fec }`

`undo port fec mode`

Default

The FEC mode of an interface is autonegotiated.

Views

100-GE interface view

Predefined user roles

network-admin

Parameters

`auto`: Specifies the FEC autonegotiation mode.

`none`: Performs no FEC.

`rs-fec`: Specifies the RS-FEC mode.

Usage guidelines

The FEC feature corrects packet errors to improve transmission quality. It attaches correction information to a packet at the sending end, and corrects error codes generated during transmission at the receiving end based on the correction information. You can set the FEC mode as needed.

Make sure you set the same FEC mode for both interfaces of a link.

A 100-GE interface not operating at 100 Gbps does not support FEC mode configuration.

Examples

Set the FEC mode of HundredGigE1/0/54 to autonegotiation.

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/54
[Sysname-HundredGigE1/0/54] port fec mode auto
```

New feature: Displaying ND entry statistics

Displaying ND entry statistics

As from this release, the device supports displaying ND entry statistics.

Command reference

display ipv6 neighbors statistics

Use **display ipv6 neighbors statistics** to display ND entry statistics.

Syntax

display ipv6 neighbors statistics { [**by-slot**] **all** | **interface** { *interface-name* | *interface-type interface-number* } | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays statistics about all ND entries.

interface interface-type interface-number: Specifies an interface by its type and number.

by-slot: Displays ND entry statistics on a per member device basis.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ND entry statistics for all member devices.

Usage guidelines

Use ND entry statistics to monitor the usage of entry resources. When an error occurs during packet forwarding, you can view ND entry statistics to identify whether it is because too many entry resources are occupied.

Examples

Display ND entry statistics on Ten-GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 neighbors statistics interface ten-gigabitethernet 1/0/1
----------------------------------------------
State      Dynamic      Static      Rule
----------------------------------------------
Incmp      0            0           0
Reach      0            2           0
Stale      1            -           -
Delay      0            -           -
Probe      0            -           -
----------------------------------------------
Total      1            2           0
```

Display statistics about all ND entries.

```
<Sysname> display ipv6 neighbors statistics all
----------------------------------------------
State      Dynamic      Static      Rule
----------------------------------------------
Incmp      0             4             0
Reach      1             2             0
Stale      0             -             -
Delay      0             -             -
Probe      0             -             -
----------------------------------------------
Total      1             6             0
```

Table 1 Command output

Field	Description
Dynamic	Number of ND entries obtained dynamically.
Static	Number of ND entries configured statically.
Rule	Number of ND entries obtained from the IPoE or Portal module.
Incmp	Number of ND entries in **Incmp** state.
Reach	Number of ND entries in **Reach** state.
Stale	Number of ND entries in **Stale** state.
Delay	Number of ND entries in **Delay** state.
Probe	Number of ND entries in **Probe** state.

New feature: User IP address conflict SNMP notifications for ARP

Enabling user IP address conflict SNMP notifications for ARP

About this task

When a user IP address conflict occurs, this feature enables the device to send a notification to the SNMP module. The notification includes the sender IP address and sender MAC address in the conflicted ARP packet and the MAC address in the corresponding local ARP entry.

For user IP address conflict notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.
   `system-view`
2. Enable user IP address conflict SNMP notifications for ARP.
   `snmp-agent trap enable arp user-ip-conflict`
   By default, user IP address conflict SNMP notifications for ARP are disabled.

Command reference

Modified command: snmp-agent trap enable arp

Old syntax

`snmp-agent trap enable arp` [**`rate-limit`**]

`undo snmp-agent trap enable arp` [**`rate-limit`**]

New syntax

`snmp-agent trap enable arp` [**`rate-limit`** | **`user-ip-conflict`**] *

`undo snmp-agent trap enable arp` [**`rate-limit`** | **`user-ip-conflict`**] *

Views

System view

Change description

The **`user-ip-conflict`** keyword was added. This keyword enables user IP address conflict SNMP notifications for ARP. If you do not specify a keyword in this command, this command enables all types of SNMP notifications for ARP.

New feature: Interface alarm functions

Configuring interface alarm functions

About this task

With the interface alarm functions enabled, when the number of error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of error packets on

an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

Restrictions and guidelines

You can configure the interface alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

An interface that is shut down because of error packet alarms cannot automatically recover. To bring up the interface, execute the **undo shutdown** command on the interface.

Enabling interface alarm functions

1. Enter system view.

   system-view

2. Enable alarm functions for the interface monitoring module.

   snmp-agent trap enable ifmonitor [**crc-error** | **input-error** | **input-usage** | **output-error** | **output-usage**] *

   By default, all alarm functions are enabled for interfaces.

Configuring CRC error packet parameters

1. Enter system view.

   system-view

2. Configure global CRC error packet alarm parameters.

   ifmonitor crc-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

   By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packets.

3. Enter Ethernet interface view.

   interface *interface-type interface-number*

4. Configure CRC error packet alarm parameters for the interface.

   port ifmonitor crc-error [**ratio**] **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

   By default, an interface uses the global CRC error packet alarm parameters.

Configuring input error packet alarm parameters

1. Enter system view.

   system-view

2. Configure global input error packet alarm parameters.

   ifmonitor input-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

   By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packets.

3. Enter Ethernet interface view.

   interface *interface-type interface-number*

4. Configure input error packet alarm parameters for the interface.

   port ifmonitor input-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

By default, an interface uses the global input error packet alarm parameters.

Configuring output error packet alarm parameters

1. Enter system view.

   system-view

2. Configure global output error packet alarm parameters.

   ifmonitor output-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

   By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packets.

3. Enter Ethernet interface view.

   interface *interface-type interface-number*

4. Configure output error packet alarm parameters.

   port ifmonitor output-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

   By default, an interface uses the global output error packet alarm parameters.

Configuring input bandwidth usage alarm parameters

1. Enter system view.

   system-view

2. Configure global input bandwidth usage alarm parameters.

   ifmonitor input-usage slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value*

   By default, the upper threshold is 90 and the lower threshold is 80 for input bandwidth usage alarms.

3. Enter Ethernet interface view.

   interface *interface-type interface-number*

4. Configure input bandwidth usage alarm parameters.

   port ifmonitor input-usage high-threshold *high-value* **low-threshold** *low-value*

   By default, an interface uses the global input bandwidth usage alarm parameters.

Configuring output bandwidth usage alarm parameters

1. Enter system view.

   system-view

2. Configure global output bandwidth usage alarm parameters.

   ifmonitor output-usage slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value*

   By default, the upper threshold is 90 and the lower threshold is 80 for output bandwidth usage alarms.

3. Enter Ethernet interface view.

   interface *interface-type interface-number*

4. Configure output bandwidth usage alarm parameters.

   port ifmonitor output-usage high-threshold *high-value* **low-threshold** *low-value*

   By default, an interface uses the global output bandwidth usage alarm parameters.

Command reference

ifmonitor crc-error

Use **ifmonitor crc-error** to configure global CRC error packet alarm parameters.

Use **undo ifmonitor crc-error** to restore the default.

Syntax

ifmonitor crc-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor crc-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor crc-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor input-error

Use **ifmonitor input-error** to configure global input error packet alarm parameters.

Use **undo ifmonitor input-error** to restore the default.

Syntax

ifmonitor input-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor input-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.

- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor input-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor input-usage

Use **ifmonitor input-usage** to configure global input bandwidth usage alarm parameters.

Use **undo ifmonitor input-usage** to restore the default.

Syntax

ifmonitor input-usage slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value*

undo ifmonitor input-usage slot *slot-number*

Default

The upper threshold is 90, and the lower threshold is 80.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input bandwidth usage alarms, in the range of 1 to 100.

low-threshold *low-value*: Specifies the lower threshold for input bandwidth usage alarms, in the range of 1 to 100.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the input bandwidth usage alarm function enabled, when the input bandwidth usage on an interface in normal state within the most recent statistics polling interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the input bandwidth usage on an interface in the alarm state within the most recent statistics polling interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

To set the statistics polling interval, use the **flow-interval** command.

You can configure the input bandwidth usage alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

For this command to take effect, you must use the **snmp-agent trap enable ifmonitor** command to enable the input bandwidth usage alarm function.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 95 and lower threshold to 80 for input bandwidth usage alarms.

```
<Sysname> system-view
[Sysname] ifmonitor input-usage slot 1 high-threshold 95 low-threshold 80
```

Related commands

flow-interval

snmp-agent trap enable ifmonitor

ifmonitor output-error

Use **ifmonitor output-error** to configure global output error packet alarm parameters.

Use **undo ifmonitor output-error** to restore the default.

Syntax

ifmonitor output-error slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo ifmonitor output-error slot *slot-number*

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of

output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms.

```
<Sysname> system-view
[Sysname] ifmonitor output-error slot 1 high-threshold 5000 low-threshold 400 interval
6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor output-usage

Use **ifmonitor output-usage** to configure global output bandwidth usage alarm parameters.

Use **undo ifmonitor output-usage** to restore the default.

Syntax

ifmonitor output-usage slot *slot-number* **high-threshold** *high-value* **low-threshold** *low-value*

undo ifmonitor output-usage slot *slot-number*

Default

The upper threshold is 90, and the lower threshold is 80.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output bandwidth usage alarms, in the range of 1 to 100.

low-threshold *low-value*: Specifies the lower threshold for output bandwidth usage alarms, in the range of 1 to 100.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the output bandwidth usage alarm function enabled, when the output bandwidth usage on an interface in normal state within the most recent statistics polling interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the output bandwidth usage on an interface in the alarm state within the most recent statistics polling interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

To set the statistics polling interval, use the **flow-interval** command.

You can configure the output bandwidth usage alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

For this command to take effect, you must use the **snmp-agent trap enable ifmonitor** command to enable the output bandwidth usage alarm function.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 80 and lower threshold to 60 for output bandwidth usage alarms.

```
<Sysname> system-view
[Sysname] ifmonitor output-usage slot 1 high-threshold 80 low-threshold 60
```

Related commands

flow-interval

snmp-agent trap enable ifmonitor

port ifmonitor crc-error

Use **port ifmonitor crc-error** to configure CRC error packet alarm parameters for an interface.

Use **undo port ifmonitor crc-error** to restore the default.

Syntax

port ifmonitor crc-error [**ratio**] **high-threshold** *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor crc-error

Default

An interface uses the global CRC error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ratio: Specifies the alarm thresholds in percentage. If you do not specify this keyword, you configure the alarm thresholds in absolute value.

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms. If you specify the **ratio** keyword, the value range is 1 to 100. If you do not specify the **ratio** keyword, the value range is 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms. If you specify the **ratio** keyword, the value range is 1 to 100. If you do not specify the **ratio** keyword, the value range is 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port ifmonitor crc-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor input-error

Use **port ifmonitor input-error** to configure input error packet alarm parameters for an interface.

Use **undo port ifmonitor input-error** to restore the default.

Syntax

port ifmonitor input-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor input-error

Default

An interface uses the global input error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port ifmonitor input-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor input-usage

Use **port ifmonitor input-usage** to configure input bandwidth usage alarm parameters.

Use **undo port ifmonitor input-usage** to restore the default.

Syntax

port ifmonitor input-usage high-threshold *high-value* **low-threshold** *low-value*

undo port ifmonitor input-usage

Default

An interface uses the global input bandwidth usage alarm parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input bandwidth usage alarms, in the range of 1 to 100.

low-threshold *low-value*: Specifies the lower threshold for input bandwidth usage alarms, in the range of 1 to 100.

Usage guidelines

With the input bandwidth usage alarm function enabled, when the input bandwidth usage on an interface in normal state within the most recent statistics polling interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the input bandwidth usage on an interface in the alarm state within the most recent statistics polling interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

To set the statistics polling interval, use the **flow-interval** command.

You can configure the input bandwidth usage alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

For this command to take effect, you must use the **snmp-agent trap enable ifmonitor** command to enable the input bandwidth usage alarm function.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 80 and lower threshold to 60 for input bandwidth usage alarms on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port ifmonitor input-usage high-threshold 80
low-threshold 60
```

Related commands

flow-interval

snmp-agent trap enable ifmonitor

port ifmonitor output-error

Use **port ifmonitor output-error** to configure output error packet alarm parameters for an interface.

Use **undo port ifmonitor output-error** to restore the default.

Syntax

port ifmonitor output-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor output-error

Default

An interface uses the global output error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port ifmonitor output-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor output-usage

Use **port ifmonitor output-usage** to configure output bandwidth usage alarm parameters.

Use **undo port ifmonitor output-usage** to restore the default.

Syntax

port ifmonitor output-usage high-threshold *high-value* **low-threshold** *low-value*

undo port ifmonitor output-usage

Default

An interface uses the global output bandwidth usage alarm parameters.

Views

Interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output bandwidth usage alarms, in the range of 1 to 100.

low-threshold *low-value*: Specifies the lower threshold for output bandwidth usage alarms, in the range of 1 to 100.

Usage guidelines

With the output bandwidth usage alarm function enabled, when the output bandwidth usage on an interface in normal state within the most recent statistics polling interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the output bandwidth usage on an interface in the alarm state within the most recent statistics polling interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

To set the statistics polling interval, use the **flow-interval** command.

You can configure the output bandwidth usage alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

For this command to take effect, you must use the **snmp-agent trap enable ifmonitor** command to enable the output bandwidth usage alarm function.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 9 and lower threshold to 7 for output bandwidth usage alarms on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port ifmonitor output-usage high-threshold 9
low-threshold 7
```

Related commands

flow-interval

snmp-agent trap enable ifmonitor

snmp-agent trap enable ifmonitor

Use **snmp-agent trap enable ifmonitor** to enable interface alarm functions.

Use **undo snmp-agent trap enable ifmonitor** to disable interface alarm functions.

Syntax

snmp-agent trap enable ifmonitor [**crc-error** | **input-error** | **input-usage** | **output-error** | **output-usage**] *

undo snmp-agent trap enable ifmonitor [**crc-error** | **input-error** | **input-usage** | **output-error** | **output-usage**] *

Default

Interface alarm functions are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

crc-error: Enables the CRC error packet alarm function for interfaces.

input-error: Enables the input error packet alarm function for interfaces.

input-usage: Enables the input bandwidth usage alarm function for interfaces.

output-error: Enables the output error packet alarm function for interfaces.

output-usage: Enables the output bandwidth usage alarm function for interfaces.

Examples

Enable the CRC error packet alarm function for interfaces.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ifmonitor crc-error
```

New feature: Advertising only the global unicast address in the NEXT_HOP attribute

Advertising only the global unicast address in the NEXT_HOP attribute

About this task

An IPv6 peer might fail to learn routes if it cannot parse a route update that contains both the link-local address and the global unicast address. To resolve this issue, perform this task to enable the local device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

Restrictions and guidelines

This feature might not apply to EBGP peers established through directly connected broadcast interfaces. If the next hop of the advertised route and the directly connected broadcast interfaces belong to the same subnet, this feature does not take effect.

Procedure (IPv4 unicast address family)

1. Enter system view.

   system-view

2. Enter BGP IPv4 unicast address family view or BGP-VPN IPv4 unicast address family view.

- Execute the following commands in sequence to enter BGP IPv4 unicast address family view:

  bgp *as-number* [**instance** *instance-name*]

  address-family ipv4 [**unicast**]

- Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:

  bgp *as-number* [**instance** *instance-name*]

  ip vpn-instance *vpn-instance-name*

  address-family ipv4 [**unicast**]

3. Enable the device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

   nexthop global-address-only

   By default, the local device with a link-local address advertises both the link-local address and the global unicast address in the NEXT_HOP attribute to IPv6 BGP peers.

Procedure (IPv6 unicast/multicast address family)

1. Enter system view.

   system-view

2. Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.

   - Execute the following commands in sequence to enter BGP IPv6 unicast address family view:

     bgp *as-number* [**instance** *instance-name*]

     address-family ipv6 [**unicast**]

   - Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:

     bgp *as-number* [**instance** *instance-name*]

     ip vpn-instance *vpn-instance-name*

     address-family ipv6 [**unicast**]

   - Execute the following commands in sequence to enter BGP IPv6 multicast address family view:

     bgp *as-number* [**instance** *instance-name*]

     address-family ipv6 multicast

3. Enable the device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

   nexthop global-address-only

   By default, the local device with a link-local address advertises both the link-local address and the global unicast address in the NEXT_HOP attribute to IPv6 BGP peers.

Command reference

nexthop global-address-only

Use **nexthop global-address-only** to enable the device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

Use **undo nexthop global-address-only** to restore the default.

Syntax

nexthop global-address-only

undo nexthop global-address-only

Default

The local device with a link-local address advertises both the link-local address and the global unicast address in the NEXT_HOP attribute to IPv6 BGP peers.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv6 multicast address family view

Predefined user roles

network-admin

Usage guidelines

An IPv6 peer might fail to learn routes if it cannot parse a route update that contains both the link-local address and the global unicast address. To resolve this issue, execute this command to enable the local device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

This command might not apply to EBGP peers established through directly connected broadcast interfaces. If the next hop of the advertised route and the directly connected broadcast interfaces belong to the same subnet, this command does not take effect.

Examples

In BGP IPv6 unicast address family view, enable the device to advertise only the global unicast address in the NEXT_HOP attribute to its IPv6 peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 unicast
[Sysname-bgp-default-ipv6] nexthop global-address-only
```

New feature: IPv6 duplicate detection on duplicate addresses

Enabling duplicate detection on duplicate addresses

About this task

If the system detects that an IPv6 address on an interface has been used on the network, the device marks that IPv6 address as duplicate. The interface cannot use the address for communication.

By default, an interface does not perform duplicate detection on duplicate addresses. Once an IPv6 address is marked as duplicate on an interface, it will be unusable even after it becomes unique on the link later.

To resolve this issue, enable duplicate detection for duplicate addresses. This feature regularly sends NS messages to the duplicate address until it does not receive an NA response message from that address or until duplicate detection is disabled for duplicate addresses.

You can set the maximum duplicate detection interval for duplicate addresses. After the device marks a detected address as duplicate, it waits for a random amount of time between 1 and the maximum detection interval. Then, the device resends an NS message to the solicited-node multicast address of the duplicate address. This mechanism helps reduce the risk of congestion that results from the NS messages sent for duplicate detection.

Procedure

1. Enter system view.
   `system-view`
2. Enable duplicate detection on duplicate addresses.
   `ipv6 address duplicate-detect enable`
   By default, duplicate detection is disabled on duplicate addresses.
3. (Optional.) Set the maximum duplicate detection interval for duplicate addresses.
   `ipv6 address duplicate-detect interval` *`interval`*
   By default, the maximum duplicate detection interval for duplicate addresses is 5 seconds.

Command reference

ipv6 address duplicate-detect enable

Use **`ipv6 address duplicate-detect enable`** to enable duplicate detection on duplicate addresses.

Use **`undo ipv6 address duplicate-detect enable`** to disable duplicate detection on duplicate addresses.

Syntax

`ipv6 address duplicate-detect enable`

`undo ipv6 address duplicate-detect enable`

Default

Duplicate detection is disabled on duplicate addresses.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If the system detects that an IPv6 address on an interface has been used on the network, the device marks that IPv6 address as duplicate. The interface cannot use the address for communication.

By default, an interface does not perform duplicate detection for duplicate addresses. Once an IPv6 address is marked as duplicate on an interface, it will be unusable even after it becomes unique on the link later.

To resolve this issue, enable duplicate detection on duplicate addresses. This feature regularly sends NS messages to the duplicate address until it does not receive an NA response message from that address or until duplicate detection is disabled on duplicate addresses.

To set the maximum duplicate detection interval for duplicate addresses, use the **`ipv6 address duplicate-detect interval`** command.

For more information about duplicate address detection, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

Examples

Enable duplicate detection on duplicate addresses.

```
<Sysname> system-view
[Sysname] ipv6 address duplicate-detect enable
```

Related commands

ipv6 address duplicate-detect interval

ipv6 address duplicate-detect interval

Use **ipv6 address duplicate-detect interval** to set the maximum duplicate detection interval for duplicate addresses.

Use **undo ipv6 address duplicate-detect interval** to restore the default.

Syntax

ipv6 address duplicate-detect interval *interval*

undo ipv6 address duplicate-detect *interval*

Default

The maximum duplicate detection interval for duplicate addresses is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Sets the maximum duplicate detection interval for duplicate addresses in seconds. The value range for this argument is 1 to 60.

Usage guidelines

You can set the maximum duplicate detection interval for duplicate addresses. After the device marks a detected address as duplicate, it waits for a random amount of time between 1 and the maximum detection interval. Then, the device resends an NS message to the solicited-node multicast address of the duplicate address. This mechanism helps reduce the risk of congestion that results from the NS messages sent for duplicate detection.

Examples

Set the maximum duplicate detection interval to 10 seconds for duplicate addresses.

```
<Sysname> system-view
[Sysname] ipv6 address duplicate-detect interval 10
```

Related commands

ipv6 address duplicate-detect enable

New feature: BGP route re-origination

Configuring BGP route re-origination

About this task

If the route target of a received VPNv4/VPNv6 route matches the import route target of the local VPN instance, the local VPN instance re-originates the route and advertises the re-originated route to VPNv4/VPNv6 peers.

Configuring route re-origination

1. Enter system view.

   system-view
2. Enter BGP instance view.

   bgp as-number [***instance instance-name***]
3. Enter BGP-VPN instance view.

   ip vpn-instance ***vpn-instance-name***
4. Enter BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view.
   - Enter BGP-VPN IPv4 unicast address family view.

     address-family ipv4 [**unicast**]
   - Enter BGP-VPN IPv6 unicast address family view.

     address-family ipv6 [**unicast**]
5. Configure the VPN instance to re-originate the optimal route and advertise the re-originated route to VPNv4/VPNv6 peers.

   advertise route-reoriginate [**route-policy** *route-policy-name*] [**replace-rt**]

   By default, the VPN instance does not advertise a received route to VPNv4/VPNv6 peers.

Command reference

advertise route-reoriginate

Use **advertise route-reoriginate** to configure a VPN instance to re-originate the optimal route and advertise the re-originated route to VPNv4/VPNv6 peers.

Use **undo advertise route-reoriginate** to cancel the configuration.

Syntax

advertise route-reoriginate [**route-policy** *route-policy-name*] [**replace-rt**]

undo advertise route-reoriginate

Default

A VPN instance does not advertise a received route to VPNv4/VPNv6 peers.

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy to filter VPNv4/VPNv6 routes to be advertised to VPNv4/VPNv6 peers. The *route-policy-name* argument specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify this option, the command advertises all VPNv4/VPNv6 routes to VPNv4/VPNv6 peers.

replace-rt: Uses the route target of the local VPN instance to replace the route target of the VPNv4/VPNv6 route. If you do not specify this keyword, the route target of the route will not be changed.

Usage guidelines

If the route target of a received VPNv4/VPNv6 route matches the import route target of the local VPN instance, the local VPN instance re-originates the route and advertises the re-originated route to VPNv4/VPNv6 peers.

Examples

In BGP-VPN IPv4 unicast address family view, configure VPN instance **vpn1** to re-originate the optimal route and advertise the re-originated route to VPNv4 peers

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1] address-family ipv4
[Sysname-bgp-default-ipv4-vpn1] advertise route-reoriginate
```

New feature: Establishing neighbors through the secondary IP address of an interface

Enabling OSPF to establish neighbors through the secondary IP address of an interface

About this task

By default, OSPF uses the primary IP address of an interface to establish neighbors. You can configure this feature to enable OSPF to establish neighbors through the secondary IP address of an interface.

Restrictions and guidelines

- If an interface has both primary and secondary addresses and you have advertised the network that contains the primary address in an area of an OSPF process, OSPF uses the primary address to establish neighbors. For OSPF to establish neighbors through the secondary IP addresses, you must advertise the networks to which these addresses belong in the same area of the same OSPF process.
- If an interface does not have a primary address but has multiple secondary addresses, OSPF uses the lowest secondary address to establish neighbors. For OSPF to establish neighbors through the other secondary addresses, you must advertise the networks to which these addresses belong in the same area of the same OSPF process.
- OSPF cannot use secondary addresses for neighbor establishment on a P2P link if the local and remote addresses of the link belong to different networks.

Procedure

1. Enter system view.
   system-view
2. Enter OSPF view.
   ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *
3. Enter interface view.
   interface *interface-type interface-number*
4. Enable OSPF to establish neighbors through the secondary IP address of the interface.
   ospf peer sub-address enable

Command reference

New command: ospf peer sub-address enable

Use **ospf peer sub-address enable** to enable OSPF to establish neighbors through the secondary IP address of an interface.

Use **undo ospf peer sub-address enable** to disable OSPF from establishing neighbors through the secondary IP address of an interface.

Syntax

ospf peer sub-address enable

undo ospf peer sub-address enable

Default

OSPF cannot establish neighbors through the secondary IP address of an interface.

Views

Interface

Predefined user roles

network-admin

Usage guidelines

By default, OSPF uses the primary IP address of an interface to establish neighbors. You can execute this command to enable OSPF to establish neighbors through both the primary and secondary IP addresses of an interface.

If an interface has both primary and secondary addresses and you have advertised the network that contains the primary address in an area of an OSPF process, OSPF uses the primary address to establish neighbors. For OSPF to establish neighbors through the secondary IP addresses, you must advertise the networks to which these addresses belong in the same area of the same OSPF process.

If an interface does not have a primary address but has multiple secondary addresses, OSPF uses the lowest secondary address to establish neighbors. For OSPF to establish neighbors through the other secondary addresses, you must advertise the networks to which these addresses belong in the same area of the same OSPF process.

OSPF cannot use secondary addresses for neighbor establishment on a P2P link if the local and remote addresses of the link belong to different networks.

Examples

On interface VLAN-interface 10, enable OSPF to establish neighbors through the secondary IP address of the interface.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf peer sub-address enable
```

Related commands

network

ospf area

Modified command: display ospf interface

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

Change description

The **Interface Address Type** field is added to the output of the **display ospf interface** command to display whether a neighbor is established through the primary or secondary IP address.

Modified feature: IPv6 routes with prefixes longer than 64 bits

Feature change description

Before modification: By default, The device does not support for IPv6 routes with prefixes longer than 64 bits.

After modification: By default, The device supports for IPv6 routes with prefixes longer than 64 bits.

Command changes

Modified command: hardware-resource routing-mode

Syntax

hardware-resource routing-mode { **ipv6-64** | **ipv6-128** }

.Views

System view

Change description

Before modification: By default, The device does not support for IPv6 routes with prefixes longer than 64 bits.

After modification: By default, The device supports for IPv6 routes with prefixes longer than 64 bits.

Modified feature: Match criteria in a traffic class

Feature change description

As from this version, you can configure a match criterion to match the input interface of packets in a traffic class.

Modified command: if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Views

Traffic class view

Change description

Before modification: You cannot configure a match criterion to match the input interface of packets.

After modification: You can configure a match criterion to match the input interface of packets by specifying the **inbound-interface** *interface-type interface-number* option for the *match-criteria* argument.

Table 2 Available match criteria

Option	Description
inbound-interface *interface-type interface-number*	Matches an input interface specified by its type and number. If this option is configured in a traffic class with logic AND operator, the traffic class is no longer in effect after the subcard where the input interface resides is removed. After the removed subcard is reinserted, the traffic class takes effect again. If you do not reinsert the subcard, you must delete this traffic class and configure it again as needed. Otherwise, even if you add other match criteria to the traffic class, the traffic class does not take effect again.

Modified feature: Associating a traffic behavior with a traffic class

Feature change description

As from this version, you can associate a traffic behavior with a traffic class in loose mode. The loose mode takes effect only when you apply a QoS policy to the control plane.

The loose mode can match those packets that cannot be identified, such as ARP packets. Use the loose mode with caution, because it might mistakenly match protocol packets.

Follow these steps to use the loose mode to rate limit the packets of the specified protocol received on the specified interface and sent to the control plane:

1. Create an ACL, and create a rule that matches packets of the specified protocol in the ACL.
2. Create a traffic class with logic AND operator, and configure the **if-match acl** and **if-match inbound-interface** criteria in the traffic class.
3. Create a traffic behavior and configure actions in it.

4. Create a QoS policy, and specify the **mode loose** keyword when you associate the traffic behavior with the traffic class configured above.
5. Apply the QoS to the control plane.

Protocol packets of the specified protocol received on any other interfaces are still rate limited by the protocol packet rate limiting feature when they are sent to the control plane.

Command changes

Modified command: classifier behavior

Old syntax

classifier *classifier-name* **behavior** *behavior-name* [**mode** { **dcbx** | **qppb-manipulation** } | **insert-before** *before-classifier-name*]

New syntax

classifier *classifier-name* **behavior** *behavior-name* [**mode** { **dcbx** | **loose** | **qppb-manipulation** } | **insert-before** *before-classifier-name*]

Views

QoS policy view

Change description

Before modification: You cannot associate a traffic behavior with a traffic class in loose mode

After modification: You can associate a traffic behavior with a traffic class in loose mode

Modified feature: Displaying the running configuration

Feature change description

As from this release, the running configuration can be displayed by section.

Command changes

Modified command: display current-configuration

Old syntax

display current-configuration [[**configuration** [*module-name*] | **exclude-provision** | **interface** [*interface-type* [*interface-number*]]] [**all**] | **slot** *slot-number*]

New syntax

display current-configuration [[**configuration** [*module-name*] | **exclude-provision** | **interface** [*interface-type* [*interface-number*]]] [**all**] | **slot** *slot-number*] [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

The following parameters are added to this command:

by-section: Displays the running configuration by section. Each section contains the configuration in a command view and two adjacent sections are separated by a pound sign (#). If you do not specify this keyword, the command displays the running configuration by line.

begin: Displays the first configuration section that matches the specified regular expression and all subsequent configuration sections.

exclude: Displays all configuration sections not matching the specified regular expression.

include: Displays all configuration sections matching the specified regular expression.

regular-expression: Specifies a regular expression to filter the configuration sections, a case-sensitive string of 1 to 256 characters. A section matches the specified regular expression if it contains command lines that match the specified regular expression.

Modified feature: Displaying the contents of the configuration file for the next system startup

Feature change description

As from this release, the contents of the configuration file for the next system startup can be displayed by section.

Command changes

Modified command: display saved-configuration

Old syntax

display saved-configuration

New syntax

display saved-configuration [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

Views

Any view

Change description

The following parameters are added to this command after modification:

by-section: Displays the configuration used at the next startup by section. Each section contains the configuration in a command view and two adjacent sections are separated by a pound sign (#). If you do not specify this keyword, the command displays the configuration used at the next startup by line.

begin: Displays the first configuration section that matches the specified regular expression and all subsequent configuration sections.

exclude: Displays all configuration sections not matching the specified regular expression.

include: Displays all configuration sections matching the specified regular expression.

regular-expression: Specifies a regular expression to filter the configuration sections, a case-sensitive string of 1 to 256 characters. A section matches the specified regular expression if it contains command lines that match the specified regular expression.

Modified feature: Optimized display of BGP BMP server information

Feature change description

As from this release, the output of the **display bgp bmp server** command includes the following information:

- Interval at which BGP sends statistics information to the BMP server.
- Type of the routes that BGP reports to the BMP server.
- Whether the BMP client sends peer up notifications with mode flags to the BMP server.
- Whether the BMP client sends peer down notifications with mode flags to the BMP server.

Command changes

Modified command: display bgp bmp server

Syntax

display bgp [**instance** *instance-name*] **bmp server** *server-number*

Views

Any view

Change description

After modification, the following fields are added to the output of this command:

- **Statistics report interval**: Interval (in seconds) at which BGP sends statistics information to the BMP server.
- **Reported route mode**: Type of routes that BGP sends to the BMP server:

  - **adj-rib-in**—Send routes received from the monitored peer or peer group to the BMP server.
  - **adj-rib-out**—Send routes advertised to the monitored peer or peer group to the BMP server.
  - **pre-policy**—Send routes to the BMP server without route filtering.
  - **post-policy**—Send routes to the BMP server after route filtering.
  - **both**—Send both filtered and unfiltered routes to the BMP server.
  - **loc-rib**—Send the optimal routes in the routing table to the BMP server.

- **Pu-monitor-mode**: Whether the peer up notifications that the BMP client sends to the BMP server carry the mode flag.

  - **Enabled**—Carry the mode flag.
  - **Disabled**—Do not carry the mode flag.

- **Pd-monitor-mode**: Whether the peer down notifications that the BMP client sends to the BMP server carry the mode flag.

  - **Enabled**—Carry the mode flag.
  - **Disabled**—Do not carry the mode flag.

Examples

Display information about BMP server 1.

```
<Sysname> display bgp bmp server 1
BMP server number: 1
Server VPN instance name: vpna
```

```
Server address: 100.1.1.1  Server port: 6895
Client address: 100.1.1.2  Client port: 21452
BMP server state: Connected  Up for 00h41m53s
TCP source interface has been configured
Statistics report interval: 5s
Reported route mode: adj-rib-in pre-policy
Pu-monitor-mode: Enabled
Pd-monitor-mode: Enabled
Message statistics:
Total messages sent: 15
         INITIATION: 1
        TERMINATION: 0
       STATS-REPORT: 0
            PEER-UP: 4
          PEER-DOWN: 3
          ROUTE-MON: 7
BGP peers monitored by BMP server:
  10.1.1.1
```

Modified feature: Disabling BGP session establishment with peers and peer groups

Feature change description

As from this release, the value range for the **graceful** *graceful-time* option in the **ignore all-peers** command and the **peer ignore** command is changed. The new value range is 0 to 65535. If you set the value to 0 for the *graceful-time* argument, the device sends low-priority routes to peers or peer groups and does not tear down BGP sessions to the peers or peer groups.

Command changes

Modified command: ignore all-peers

Syntax

ignore all-peers [**graceful** *graceful-time* { **community** { *community-number* | *aa:nn* } | **local-preference** *preference* | **med** *med* } *]

Views

BGP instance view

Change description

- Before modification: The value range for the *graceful-time* argument is 60 to 65535 seconds.
- After modification: The value range for the *graceful-time* argument is 0 to 65535 seconds. If you set the value to 0 for this argument, the device does not tear down BGP sessions to peers and peer groups.

Modified command: interface-peer/peer ignore

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] | *link-local-address* **interface** *interface-type interface-number* } **ignore** [**graceful** *graceful-time* { **community** { *community-number* | *aa:nn* } | **local-preference** *preference* | **med** *med* } *]

interface-peer *interface-type interface-number* **ignore** [**graceful** *graceful-time* { **community** { *community-number* | *aa:nn* } | **local-preference** *preference* | **med** *med* } *]

Views

BGP instance view

BGP-VPN instance view

Change description

- Before modification: The value range for the *graceful-time* argument is 60 to 65535 seconds.
- After modification: The value range for the *graceful-time* argument is 0 to 65535 seconds. If you set the value to 0 for this argument, the device does not tear down BGP sessions to the specified peers or peer group.

Modified feature: Optimizations to VXLAN command output

Feature change description

In this software version, the following optimizations were made to VXLAN display commands:

- The **display l2vpn vsi** command displays both input and output packet rates for a VSI.
- The **display vxlan tunnel** command displays the total number of VXLAN tunnels for a VXLAN, the source and destination addresses of each VXLAN tunnel, and the outgoing VXLAN ID.

Command changes

Modified command: display l2vpn vsi

Syntax

display l2vpn vsi [**name** *vsi-name*] [**verbose**]

Views

Any view

Change description

The following fields were added to the command output:

- **Input Rate**: Incoming traffic rate for a VSI, in bps and pps.
- **Output Rate**: Outgoing traffic rate for a VSI, in bps and pps.

Modified command: display vxlan tunnel

Syntax

display vxlan tunnel [**vxlan-id** *vxlan-id*]

Views

Any view

Change description

The following fields were added to the command output:

- **Total number of VXLAN tunnels**: The total number of VXLAN tunnels assigned to a VXLAN.
- **Source**: Tunnel source address.
- **Destination**: Tunnel destination address.
- **Out VNI**: Remote VXLAN ID mapped to the local VXLAN ID by using the **mapping vni** command. If no remote VXLAN ID is configured, this field displays a hyphen (**-**).

Modified feature: Sharing of VSI interfaces among VSIs

Before modification: Multiple VSIs can share a VSI interface.

After modification: A VSI interface can be assigned to only one VSI.

Modified feature: Enabling L2TP for the specified protocol

Feature change description

As from this version, a Layer 2 Ethernet interface supports the **user-defined** keyword and a Layer 2 aggregate interface supports the **cdp**, **lacp**, **lldp**, **pagp**, **udld**, and **user-defined** *protocol-name* parameters when you enable L2TP for the specified protocol.

Command changes

Modified command: l2protocol tunnel dot1q

Old syntax

In Layer 2 Ethernet interface view:

l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** } **tunnel dot1q**

In Layer 2 aggregate interface view:

l2protocol { **gvrp** | **mvrp** | **pvst** | **stp** | **vtp** } **tunnel dot1q**

New syntax

In Layer 2 Ethernet interface view:

l2protocol { **cdp** | **dldp** | **eoam** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **user-defined** *protocol-name* | **vtp** } **tunnel dot1q**

In Layer 2 aggregate interface view:

l2protocol { **cdp** | **gvrp** | **lacp** | **lldp** | **mvrp** | **pagp** | **pvst** | **stp** | **udld** | **user-defined** *protocol-name* | **vtp** } **tunnel dot1q**

Change description

Before modification: A Layer 2 Ethernet interface does not support the **user-defined** keyword. A Layer 2 aggregate interface does not support the **cdp**, **lacp**, **lldp**, **pagp**, **udld**, or **user-defined** *protocol-name* parameters.

After modification: A Layer 2 Ethernet interface supports the **user-defined** keyword. A Layer 2 aggregate interface supports the **cdp**, **lacp**, **lldp**, **pagp**, **udld**, and **user-defined** *protocol-name* parameters.

cdp: Specifies CDP.

lacp: Specifies LACP.

lldp: Specifies LLDP.

pagp: Specifies PAGP.

udld: Specifies UDLD.

user-defined: Specifies a user-defined Layer 2 protocol.

Modified feature: Creating a local site

Feature change description

As from this version, the value range for the local site ID changes from 0-65535 to 0-256.

Command changes

Modified command: site

Syntax

site *site-id* [**range** *range-value*] [**default-offset** *default-offset*]

undo site *site-id*

Views

Auto-discovery VSI BGP signaling view

Change description

Before modification: The value range for the *site-id* argument is 0 to 65535.

After modification: The value range for the *site-id* argument is 0 to 256

Modified feature: Enabling link flapping protection on an interface

Feature change description

As from this version, the value ranges for the level-1 link flapping detection interval and level-1 link flapping detection threshold change, and you can configure the level-2 link flapping detection interval and level-2 link flapping detection threshold.

Command changes

Modified command: port link-flap protect enable

Old syntax

port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] *

New syntax

port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] * [**second-interval** *second-interval* **second-threshold** *second-threshold*]

Views

Ethernet interface view

Change description

Before modification: The value range for the level-1 link flapping detection interval is 10 to 60 seconds. The value range for the level-1 link flapping detection threshold is 5 to 10. You cannot configure the level-2 link flapping detection interval or level-2 link flapping detection threshold.

After modification: The value range for the level-1 link flapping detection interval is 5 to 86400 seconds. The value range for the level-1 link flapping detection threshold is 2 to 1200. You can configure the level-2 link flapping detection interval and level-2 link flapping detection threshold.

Modified feature: AAA methods in an ISP domain

Feature change description

As from this release, remote AAA methods are supported in an ISP domain:

- For default user accounting, RADIUS and HWTACACS are supported.
- For LAN user accounting, RADIUS is supported.
- For login user accounting, RADIUS and HWTACACS are supported.
- For portal user accounting, RADIUS is supported.
- For default user authentication, RADIUS, HWTACACS, and LDAP are supported.
- For LAN user authentication, RADIUS and LDAP are supported.
- For login user authentication, RADIUS, HWTACACS, and LDAP are supported.
- For portal user authentication, RADIUS and LDAP are supported.
- For default user authorization, RADIUS and HWTACACS are supported.
- For LAN user authorization, RADIUS is supported.
- For login user authorization, RADIUS and HWTACACS are supported.
- For portal user authorization, RADIUS is supported.

Command reference

Modified command: accounting default

Old syntax

In non-FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting default

In FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting default

New syntax

In non-FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting default

In FIPS mode:

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting default

Views

ISP domain view

Modified command: accounting lan-access

Old syntax

In non-FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

In FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

New syntax

In non-FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

In FIPS mode:

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** [**radius-scheme** *radius-scheme-name*] | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

Views

ISP domain view

Modified command: accounting login

Old syntax

In non-FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting login

In FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting login

New syntax

In non-FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo accounting login

In FIPS mode:

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo accounting login

Views

ISP domain view

Modified command: accounting portal

Old syntax

In non-FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting portal

In FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting portal

New syntax

In non-FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting portal

In FIPS mode:

accounting portal { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] | **local** [**radius-scheme** *radius-scheme-name*] | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting portal

Views

ISP domain view

Modified command: authentication default

Old syntax

In non-FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication default

In FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication default

New syntax

In non-FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] |

local [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication default

In FIPS mode:

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **local** [**ldap-scheme** *ldap-scheme-name*] | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication default

Views

ISP domain view

Modified command: authentication lan-access

Old syntax

In non-FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

In FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

New syntax

In non-FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

In FIPS mode:

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

Views

ISP domain view

Modified command: authentication login

Old syntax

In non-FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication login

In FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication login

New syntax

In non-FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **local** [**ldap-scheme** *ldap-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authentication login

In FIPS mode:

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **ldap-scheme** *ldap-scheme-name* [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **local** [**ldap-scheme** *ldap-scheme-name*] | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authentication login

Views

ISP domain view

Modified command: authentication portal

Old syntax

In non-FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication portal

In FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication portal

New syntax

In non-FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication portal

In FIPS mode:

authentication portal { **ldap-scheme** *ldap-scheme-name* [**local**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication portal

Views

ISP domain view

Modified command: authorization default

Old syntax

In non-FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization default

In FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization default

New syntax

In non-FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization default

In FIPS mode:

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization default

Views

ISP domain view

Modified command: authorization lan-access

Old syntax

In non-FIPS mode:

authorization lan-access { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

In FIPS mode:

authorization lan-access { **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization lan-access

New syntax

In non-FIPS mode:

authorization lan-access { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

In FIPS mode:

authorization lan-access { **local** | **radius-scheme** *radius-scheme-name* } *

undo authorization lan-access

Views

ISP domain view

Modified command: authorization login

Old syntax

In non-FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization login

In FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization login

New syntax

In non-FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] [**none**] }

undo authorization login

In FIPS mode:

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**radius-scheme** *radius-scheme-name*] [**local**] | **local** [**radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name*] * | **radius-scheme** *radius-scheme-name* [**hwtacacs-scheme** *hwtacacs-scheme-name*] [**local**] }

undo authorization login

Views

ISP domain view

Modified command: authorization portal

Old syntax

In non-FIPS mode:

authorization portal { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization portal

In FIPS mode:

authorization portal { **local** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization portal

New syntax

In non-FIPS mode:

authorization portal { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization portal

In FIPS mode:

authorization portal { **local** | **radius-scheme** *radius-scheme-name* } *

undo authorization portal

Views

ISP domain view

Modified feature: Setting the 802.1X periodic reauthentication timer

Feature change description

As from this version, the value range for the 802.1X periodic reauthentication timer was changed. The new value range is 60 to 86400 seconds.

Command changes

Modified command: dot1x timer

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **handshake-period** *handshake-period-value* | **offline-detect** *offline-detect-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **unicast-trigger quiet-period** *quiet-period-value* | **user-aging** { **auth-fail-vlan** | **auth-fail-vsi** | **critical-vlan** | **critical-vsi** | **guest-vlan** | **guest-vsi** } *aging-time-value* }

undo dot1x timer { **ead-timeout** | **handshake-period** | **offline-detect** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** | **unicast-trigger quiet-period** | **user-aging** { **auth-fail-vlan** | **auth-fail-vsi** | **critical-vlan** | **critical-vsi** | **guest-vlan** | **guest-vsi** } }

Views

System view

Change description

Before modification: The value range for the *reauth-period-value* argument was 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified command: dot1x timer reauth-period (interface view)

Syntax

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Change description

Before modification: The value range for the *reauth-period-value* argument was 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified feature: Setting the periodic MAC reauthentication timer

Feature change description

As from this version, the value range for the periodic MAC reauthentication timer was changed. The new value range is 60 to 86400 seconds.

Command changes

Modified command: mac-authentication timer (interface view)

Syntax

mac-authentication timer { **auth-delay** *auth-delay-time* | **reauth-period** *reauth-period-value* }

undo mac-authentication timer { **auth-delay** | **reauth-period** }

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Change description

Before modification: The value range for the *reauth-period-value* argument was 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified command: mac-authentication timer (system view)

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **temporary-user-aging** *aging-time-value* | **user-aging** { **critical-vlan** | **critical-vsi** | **guest-vlan** | **guest-vsi** } *aging-time-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **reauth-period** | **server-timeout** | **temporary-user-aging** | **user-aging** { **critical-vlan** | **critical-vsi** | **guest-vlan** | **guest-vsi** } }

Views

System view

Change description

Before modification: The value range for the *reauth-period-value* argument was 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified feature: Creating an SNMPv3 user

Feature change description

As from this release, you can specify the SHA224, SHA256, SHA384, and SHA512 authentication algorithm for creating an SNMPv3 user. To configure the authentication or encryption key in encrypted form, you can specify the 3DESSHA224, 3DESSHA256, 3DESSHA384, 3DESSHA512, AES192SHA224, AES192SHA256, AES192SHA384, AES192SHA512, AES256SHA224, AES256SHA256, AES256SHA384, AES256SHA512, SHA224, SHA256, SHA384, or SHA512 authentication and encryption algorithm to calculate the key from its plaintext form to encrypted form.

The 3DESSHA224, 3DESSHA256, 3DESSHA384, and 3DESSHA512 authentication and encryption algorithms are supported only in non-FIPS mode.

Command changes

Modified command: snmp-agent usm-user v3

Old syntax

In non-FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

In FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] { **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode sha** *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

New syntax

In non-FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** | **sha224** | **sha256** | **sha384** | **sha512** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** | **sha224** | **sha256** | **sha384** | **sha512** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

In FIPS mode:

- In VACM mode:

  snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] { **cipher** | **simple** } **authentication-mode** { **sha** | **sha224** | **sha256** | **sha384** | **sha512** } *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

- In RBAC mode:

  snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]] [{ **cipher** | **simple** } **authentication-mode** { **sha** | **sha224** | **sha256** | **sha384** | **sha512** } *auth-password* [**privacy-mode** { **aes128** | **aes192** | **aes256** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } | **acl ipv6** { *ipv6-acl-number* | **name** *ipv6-acl-name* }] *

  undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

Views

System view

Change description

Before modification: The SHA224, SHA256, SHA384, and SHA512 authentication algorithms are not supported.

After modification: The SHA224, SHA256, SHA384, and SHA512 authentication algorithms are supported.

Modified command: snmp-agent calculate-password

Old syntax

In non-FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **aes192md5** | **aes192sha** | **aes256md5** | **aes256sha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

In FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **aes192sha** | **aes256sha** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

New syntax

In non-FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **3dessha224** | **3dessha256** | **3dessha384** | **3dessha512** | **aes192md5** | **aes192sha** | **aes192sha224** | **aes192sha256** | **aes192sha384** | **aes192sha512** | **aes256md5** | **aes256sha** | **aes256sha224** | **aes256sha256** | **aes256sha384** | **aes256sha512** | **md5** | **sha** | **sha224** | **sha256** | **sha384** | **sha512** } { **local-engineid** | **specified-engineid** *engineid* }

In FIPS mode:

snmp-agent calculate-password *plain-password* **mode** { **aes192sha** | **aes192sha224** | **aes192sha256** | **aes192sha384** | **aes192sha512** | **aes256sha** | **aes256sha224** | **aes256sha256** | **aes256sha384** | **aes256sha512** | **sha** | **sha224** | **sha256** | **sha384** | **sha512** } { **local-engineid** | **specified-engineid** *engineid* }

Views

System view

Change description

Before modification:

- *plain-password*: Specifies an plaintext-form key. The argument is a case-sensitvie string of 1 to 64 characters.
- The 3DESSHA224, 3DESSHA256, 3DESSHA384, 3DESSHA512, AES192SHA224, AES192SHA256, AES192SHA384, AES192SHA512, AES256SHA224, AES256SHA256, AES256SHA384, AES256SHA512, SHA224, SHA256, SHA384, and SHA512 authentication and encryption algorithms are not supported in non-FIPS mode.
- The AES192SHA224, AES192SHA256, AES192SHA384, AES192SHA512, AES256SHA224, AES256SHA256, AES256SHA384, AES256SHA512, SHA224, SHA256, SHA384, and SHA512 authentication and encryption algorithms are not supported in FIPS mode.

After modification:

- *plain-password*: Specifies an plaintext-form key. The argument is a case-sensitvie string of 1 to 128 characters.

- The 3DESSHA224, 3DESSHA256, 3DESSHA384, 3DESSHA512, AES192SHA224, AES192SHA256, AES192SHA384, AES192SHA512, AES256SHA224, AES256SHA256, AES256SHA384, AES256SHA512, SHA224, SHA256, SHA384, and SHA512 authentication and encryption algorithms are supported in non-FIPS mode.
- The AES192SHA224, AES192SHA256, AES192SHA384, AES192SHA512, AES256SHA224, AES256SHA256, AES256SHA384, AES256SHA512, SHA224, SHA256, SHA384, and SHA512 authentication and encryption algorithms are supported in FIPS mode.

Modified feature: Displaying local public keys

Feature change description

The **Key length** field was added to the output for the **display public-key local public** command to indicate the key length of public keys in local key pairs, in bits.

Command changes

Modified command: display public-key local public

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]

Views

Any view

Change description

The **Key length** field was added to the output for this command to indicate the key length of public keys in local key pairs, in bits.

Modified feature: Flow-mirroring traffic to an interface

Feature change description

When you configure flow-mirroring traffic to an interface, you can configure the destination interface to send the mirrored packets to the specified reflector port. Then, the reflector port broadcasts the mirrored packets within the specified VLAN.

Command changes

Modified command: mirror-to interface

Old syntax

Syntax 1:

mirror-to interface *interface-type interface-number* [**loopback** | [**destination-ip** *destination-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id* | **vrf-instance** *vrf-name*] *]]

Syntax 2:

mirror-to interface destination-ip *destination-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id* | **vrf-instance** *vrf-name*] *

New syntax

Syntax 1:

mirror-to interface *interface-type interface-number* [**loopback** | [**destination-ip** *destination-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id* | **vrf-instance** *vrf-name*] *]]

Syntax 2:

mirror-to interface destination-ip *destination-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value* | **vlan** *vlan-id* | **vrf-instance** *vrf-name*] *

Syntax 3:

mirror-to interface *interface-type interface-number* **reflector-port** *interface-type interface-number* **strip-vlan** *vlan-id*

Views

Traffic behavior view

Parameters

reflector-port *interface-type interface-number*: Specifies a reflector port by its type and number.

strip-vlan *vlan-id*: Broadcasts mirrored packets within a VLAN specified by its ID in the range of 1 to 4094.

Change description

Syntax 3 was added.

When you use syntax 3 to configure flow-mirroring traffic to an interface, the device copies packets received on the mirroring sources to the destination interface. Then, the destination interface sends the mirrored packets to the specified reflector port, and the reflector port broadcasts the mirrored packets within the specified VLAN. This syntax is applicable only when the mirrored packets are VLAN-tagged and these packets must be sent out of the device untagged. When you use syntax 3, the specified mirroring destination interface and reflector port must be assigned to a mirroring-type service loopback group. For more information about service loopback groups, see service loopback group configuration in *Layer 2—LAN Switching Configuration Guide*.

Modified feature: Disabling the device from learning the source MAC addresses of Layer 2 protocol packets

Feature change description

Before modification: By default, the device learns the source MAC addresses of Layer 2 protocol packets.

After modification: By default, the device does not learn the source MAC addresses of Layer 2 protocol packets. The source MAC addresses cover the MAC addresses of the following Layer 2 protocol packets:

- BPDUs destined for a MAC address in the range of 0x01-80-c2-00-00-00 to 0x01-80-c2-00-00-0f.

- GARP PDUs destined for a MAC address in the range of 0x01-80-c2-00-00-20 to 0x01-80-c2-00-00-2f.
- PVST BPDUs destined for MAC address 0x01-00-0c-cc-cc-cd.

Command changes

Modified command: mac-address mac-learning pdu

Syntax

mac-address mac-learning pdu

undo mac-address mac-learning pdu

.Views

System view

Change description

Before modification: By default, the device learns the source MAC addresses of Layer 2 protocol packets.

After modification: By default, the device does not learn the source MAC addresses of Layer 2 protocol packets.

Modified feature: Specifying multiple VLAN IDs for VLAN name TLVs

Feature change description

Before modification: When you configure a port to advertise VLAN name TLVs, you can specify only one VLAN ID.

After modification: When you configure a port to advertise VLAN name TLVs, you can specify multiple VLAN IDs. This modification applies to Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

When you execute the **display lldp local-information** and **display lldp neighbor-information** commands, the command output displays information about all advertised and received VLAN name TLVs.

Command changes

Modified command: lldp tlv-enable

Old syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** |

inventory | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

New syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id-list*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** | **vlan-name** [*vlan-id-list*] | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id-list*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** [*vlan-id-list*] | **management-vid** }

- For nearest customer bridge agents:

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** |

system-name | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id-list*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** [*vlan-id-list*] | **management-vid** }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id-list*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** [*vlan-id-list*] | **management-vid** }

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Change description

Before modification: If you configure a Layer 2 Ethernet interface or Layer 2 aggregate interface to advertise VLAN name TLVs, you can specify only one VLAN.

After modification: If you configure a Layer 2 Ethernet interface or Layer 2 aggregate interface to advertise VLAN name TLVs, you can specify multiple VLAN IDs.

vlan-name [*vlan-id-list*]: Advertises VLAN name TLVs. The *vlan-id-list* argument specifies a VLAN range in the TLVs to be advertised in the format of { *vlan-id1* [**to** *vlan-id2*] }&<1-10>. The value range for the *vlan-id* argument is 1 to 4094 and the value for *vlan-id2* must be equal to or greater than the value for *vlan-id1*. &<1-10> indicates that you can specify up to 10 VLAN ID ranges. The default value for the *vlan-id-list* argument is the lowest VLAN ID on the port. If you do not specify a VLAN ID and the port is not assigned to any VLAN, the PVID of the port is advertised or the port cancels advertising all VLAN name TLVs.

Modified feature: Applying a QoS policy to an interface

Feature change description

As from this version, you can apply a QoS policy to the outbound direction of a Layer 2 aggregate interface, Layer 3 aggregate interface or subinterface.

Command changes

Modified command: qos apply policy (interface view)

Syntax

qos apply [**ipv6-matching** | **accounting** | **mirroring** | **remarking**] **policy** *policy-name* { **inbound** | **outbound** } [**share-mode**]

undo qos apply [**ipv6-matching** | **accounting** | **mirroring** | **remarking**] **policy** *policy-name* { **inbound** | **outbound** }

Views

Interface view

Change description

Before modification: You cannot apply a QoS policy to the outbound direction of a Layer 2 aggregate interface, Layer 3 aggregate interface, or Layer 3 aggregate subinterface.

After modification: You can apply a generic or IPv6-Matching QoS policy to the outbound direction of a Layer 2 aggregate interface, Layer 3 aggregate interface, or Layer 3 aggregate subinterface.

Modified feature: Configuring MAC address borrowing

Feature change description

As from this version, the device can generate an ARP or ND entry after receiving an LLDP frame containing a management address TLV on a Layer 2 aggregate interface. You can also set the source MAC address of LLDP frames in Layer 2 aggregate interface view.

Command changes

Modified command: lldp management-address

Old syntax

Layer 2 Ethernet interface view:

lldp management-address { **arp-learning** | **nd-learning** } **vlan** *vlan-id*

undo lldp management-address { **arp-learning** | **nd-learning** }

Layer 3 Ethernet interface view:

lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

undo lldp management-address { **arp-learning** | **nd-learning** }

New syntax

Layer 2 Ethernet interface view/Layer 2 aggregate interface view:

lldp management-address { **arp-learning** | **nd-learning** } **vlan** *vlan-id*

undo lldp management-address { **arp-learning** | **nd-learning** }

Layer 3 Ethernet interface view:

lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

undo lldp management-address { **arp-learning** | **nd-learning** }

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Change description

Before modification: You cannot enable generation of ARP or ND entries for received management address TLVs on a Layer 2 aggregate interface.

After modification: You can enable generation of ARP or ND entries for received management address TLVs on a Layer 2 aggregate interface.

Modified command: lldp source-mac vlan

Syntax

lldp source-mac vlan *vlan-id*

undo lldp source-mac vlan

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Layer 3 Ethernet interface view

Change description

Before modification: The device does not support setting the source MAC address of outgoing LLDP frames on a Layer 2 aggregate interface.

After modification: The device supports setting the source MAC address of outgoing LLDP frames on a Layer 2 aggregate interface.

Modified feature: Configuring the types of advertisable TLVs on a port

Feature change description

As from this version, the **interface loopback** *interface-number* option is supported in Layer 2 Ethernet interface view when you configure the types of advertisable TLVs. That is, you can specify the IP address of a loopback interface as the management address in Layer 2 Ethernet interface view.

Command changes

Modified command: lldp tlv-enable

Old syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } |

dot1-tlv { **all** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

In IRF physical interface view:

lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

New syntax

In Layer 2 Ethernet interface view:

- For nearest bridge agents:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback**

interface-number] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** } }

- For nearest non-TPMR bridge agents:

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- For nearest customer bridge agents:

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

  undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** |

link-aggregation | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

In management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** | **eee** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

In Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

In Layer 3 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** }

In IRF physical interface view:

lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

Layer 3 aggregate interface view

RF physical interface view

Change description

Before modification: The **interface loopback** *interface-number* option is not supported in Layer 2 Ethernet interface view.

After modification: The **interface loopback** *interface-number* option is supported in Layer 2 Ethernet interface view.

Modified feature: DRNI term changes

Feature change description

The name and terms were changed for the DRNI feature as follows:

- The feature name was changed to M-LAG.
- The **drni** keyword was changed to **m-lag** or **mlag**.
- The **intra-portal-port** keyword was changed to **peer-link**.
- The **ipp** keyword was changed to **peer-link**.
- The **dr** keyword was changed to **m-lag-interface**.
- The terms used in command output and log messages were changed accordingly.

Table 3 DRNI term changes

Old term	New term
DRNI	Multichassis link aggregation (M-LAG)

DR system	M-LAG system
DR interface	M-LAG interface
DRNI MAD	M-LAG MAD
DR group	M-LAG group
DR member device	M-LAG member device
DRNI virtual IP address	M-LAG virtual IP address (M-LAG VIP)
IPL	M-LAG peer link
IPP	M-LAG peer-link interface

Command changes in DRNI

Modified command: display drni consistency

Old syntax

display drni consistency { **type1** | **type2** } { **global** | **interface** *interface-type interface-number* }

New syntax

display m-lag consistency { **type1** | **type2** } { **global** | **interface** *interface-type interface-number* }

Views

Any view

Modified command: display drni consistency-check status

Old syntax

display drni consistency-check status

New syntax

display m-lag consistency-check status

Views

Any view

Modified command: display drni drcp statistics

Old syntax

display drni drcp statistics [**interface** *interface-type interface-number*]

New syntax

display m-lag drcp statistics [**interface** *interface-type interface-number*]

Views

Any view

Modified command: display drni keepalive

Old syntax

display drni keepalive

New syntax

display m-lag keepalive

Views

Any view

Modified command: display drni mad verbose

Old syntax

display drni mad verbose

New syntax

display m-lag mad verbose

Views

Any view

Modified command: display drni role

Old syntax

display drni role

New syntax

display m-lag role

Views

Any view

Modified command: display drni summary

Old syntax

display drni summary

New syntax

display m-lag summary

Views

Any view

Modified command: display drni system

Old syntax

display drni system

New syntax

display m-lag system

Views

Any view

Modified command: display drni troubleshooting

Old syntax

display drni troubleshooting [**dr** | **ipp** | **keepalive**] [**history**] [*count*]

New syntax

display m-lag troubleshooting [**m-lag-interface** | **peer-link** | **keepalive**] [**history**] [*count*]

Views

Any view

Modified command: display drni verbose

Old syntax

display drni verbose [**interface** *interface-type interface-number*]

New syntax

display m-lag verbose [**interface** *interface-type interface-number*]

Views

Any view

Modified command: display drni virtual-ip

Old syntax

display drni virtual-ip [**interface** *interface-type interface-number*]

New syntax

display m-lag virtual-ip [**interface** *interface-type interface-number*]

Views

Any view

Modified command: drni authentication key

Old syntax

drni authentication key { **simple** | **cipher** } *string*

undo drni authentication key

New syntax

m-lag authentication key { **simple** | **cipher** } *string*

undo m-lag authentication key

Views

System view

Modified command: drni auto-recovery reload-delay

Old syntax

drni auto-recovery reload-delay *delay-value*

undo drni auto-recovery reload-delay

New syntax

m-lag auto-recovery reload-delay *delay-value*

undo m-lag auto-recovery reload-delay

Views

System view

Modified command: drni consistency-check disable

Old syntax

drni consistency-check disable

undo drni consistency-check disable

New syntax

m-lag consistency-check disable

undo m-lag consistency-check disable

Views

System view

Modified command: drni consistency-check mode

Old syntax

drni consistency-check mode { **loose** | **strict** }

undo drni consistency-check mode

New syntax

m-lag consistency-check mode { **loose** | **strict** }

undo m-lag consistency-check mode

Views

System view

Modified command: drni drcp period short

Old syntax

drni drcp period short

undo drni drcp period

New syntax

m-lag drcp period short

undo m-lag drcp period

Views

Layer 2 aggregate interface view

Tunnel interface view

Modified command: drni ipp mac-address hold

Old syntax

drni ipp mac-address hold

undo drni ipp mac-address hold

New syntax

m-lag peer-link mac-address hold

undo m-lag peer-link mac-address hold

Views

System view

Modified command: drni keepalive { ip | ipv6 }

Old syntax

drni keepalive { **ip** | **ipv6** } **destination** { *ipv4-address* | *ipv6-address* } [**source** { *ipv4-address* | *ipv6-address* } | **udp-port** *udp-number* | **vpn-instance** *vpn-instance-name*] *

undo drni keepalive { **ip** | **ipv6** }

New syntax

m-lag keepalive { **ip** | **ipv6** } **destination** { *ipv4-address* | *ipv6-address* } [**source** { *ipv4-address* | *ipv6-address* } | **udp-port** *udp-number* | **vpn-instance** *vpn-instance-name*] *

undo m-lag keepalive { **ip** | **ipv6** }

Views

System view

Modified command: drni keepalive hold-time

Old syntax

drni keepalive hold-time *value*

undo drni keepalive hold-time

New syntax

m-lag keepalive hold-time *value*

undo m-lag keepalive hold-time

Views

System view

Modified command: drni keepalive interval

Old syntax

drni keepalive interval *interval* [**timeout** *timeout*]

undo drni keepalive interval

New syntax

m-lag keepalive interval *interval* [**timeout** *timeout*]

undo m-lag keepalive interval

Views

System view

Modified command: drni mad default-action

Old syntax

drni mad default-action { **down** | **none** }

undo drni mad default-action

New syntax

m-lag mad default-action { **down** | **none** }

undo m-lag mad default-action

Views

System view

Modified command: drni mad exclude interface

Old syntax

drni mad exclude interface *interface-type interface-number*

undo drni mad exclude interface *interface-type interface-number*

New syntax

m-lag mad exclude interface *interface-type interface-number*

undo m-lag mad exclude interface *interface-type interface-number*

Views

System view

Modified command: drni mad exclude logical-interfaces

Old syntax

drni mad exclude logical-interfaces

undo drni mad exclude logical-interfaces

New syntax

m-lag mad exclude logical-interfaces

undo m-lag mad exclude logical-interfaces

Views

System view

Modified command: drni mad include interface

Old syntax

drni mad include interface *interface-type interface-number*

undo drni mad include interface *interface-type interface-number*

New syntax

m-lag mad include interface *interface-type interface-number*

undo m-lag mad include interface *interface-type interface-number*

Views

System view

Modified command: drni mad persistent

Old syntax

drni mad persistent

undo drni mad persistent

New syntax

m-lag mad persistent

undo m-lag mad persistent

Views

System view

Modified command: drni mad restore

Old syntax

drni mad restore

New syntax

m-lag mad restore

Views

System view

Modified command: drni restore-delay

Old syntax

drni restore-delay *value*

undo drni restore-delay

New syntax

m-lag restore-delay *value*

undo m-lag restore-delay

Views

System view

Modified command: drni role priority

Old syntax

drni role priority *priority-value*

undo drni role priority

New syntax

m-lag role priority *priority-value*

undo m-lag role priority

Views

System view

Modified command: drni sequence enable

Old syntax

drni sequence enable

undo drni sequence enable

New syntax

m-lag sequence enable

undo m-lag sequence enable

Views

System view

Modified command: drni standalone enable

Old syntax

drni standalone enable [**delay** *delay-time*]

undo drni standalone enable [**delay**]

New syntax

m-lag standalone enable [**delay** *delay-time*]

undo m-lag standalone enable [**delay**]

Views

System view

Modified command: drni system-mac

Old syntax

drni system-mac *mac-address*

undo drni system-mac

New syntax

m-lag system-mac *mac-address*

undo m-lag system-mac

Views

System view

Modified command: drni system-number

Old syntax

drni system-number *system-number*

undo drni system-number

New syntax

m-lag system-number *system-number*

undo m-lag system-number

Views

System view

Modified command: drni system-priority

Old syntax

drni system-priority *priority*

undo drni system-priority

New syntax

m-lag system-priority *priority*

undo m-lag system-priority

Views

System view

Modified command: port drni group

Old syntax

port drni group *group-id* [**allow-single-member**]

undo port drni group

New syntax

port m-lag group *group-id* [**allow-single-member**]

undo port m-lag group

Views

Layer 2 aggregate interface view

Modified command: port drni intra-portal-port

Old syntax

port drni intra-portal-port *port-id*

undo port drni intra-portal-port

New syntax

port m-lag peer-link *port-id*

undo port m-lag peer-link

Views

Layer 2 aggregate interface view

Tunnel interface view

Modified command: port drni ipv6 virtual-ip

Old syntax

VLAN interface view:

port drni ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] [**virtual-mac** *mac-address*] | **link-local** }

undo port drni ipv6 virtual-ip [*ipv6-address*]

Loopback interface view:

port drni ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] | **link-local** }

undo port drni ipv6 virtual-ip [*ipv6-address*]

VSI interface view:

port drni ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] | **link-local** }

undo port drni ipv6 virtual-ip [*ipv6-address*]

New syntax

VLAN interface view:

port m-lag ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] [**virtual-mac** *mac-address*] | **link-local** }

undo port m-lag ipv6 virtual-ip [*ipv6-address*]

Loopback interface view:

port m-lag ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] | **link-local** }

undo port m-lag ipv6 virtual-ip [*ipv6-address*]

VSI interface view:

port m-lag ipv6 virtual-ip *ipv6-address* { *prefix-length* [**active** | **standby**] | **link-local** }

undo port m-lag ipv6 virtual-ip [*ipv6-address*]

Views

VLAN interface view

Loopback interface view

VSI interface view

Modified command: port drni system-mac

Old syntax

port drni system-mac *mac-address*

undo port drni system-mac

New syntax

port m-lag system-mac *mac-address*

undo port m-lag system-mac

Views

Aggregate interface view

Modified command: port drni system-priority

Old syntax

port drni system-priority *priority*

undo port drni system-priority

New syntax

port m-lag system-priority *priority*

undo port m-lag system-priority

Views

Aggregate interface view

Modified command: port drni virtual-ip

Old syntax

VLAN interface view:

port drni virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**] **virtual-mac** *mac-address*

undo port drni virtual-ip [*ipv4-address*]

Loopback interface view:

port drni virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port drni virtual-ip [*ipv4-address*]

VSI interface view:

port drni virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port drni virtual-ip [*ipv4-address*]

New syntax

VLAN interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**] **virtual-mac** *mac-address*

undo port m-lag virtual-ip [*ipv4-address*]

Loopback interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port m-lag virtual-ip [*ipv4-address*]

VSI interface view:

port m-lag virtual-ip *ipv4-address* { *mask-length* | *mask* } [**active** | **standby**]

undo port m-lag virtual-ip [*ipv4-address*]

Views

VLAN interface view

Loopback interface view

VSI interface view

Modified command: reset drni drcp statistics

Old syntax

reset drni drcp statistics [**interface** *interface-list*]

New syntax

reset m-lag drcp statistics [**interface** *interface-list*]

Views

User view

Modified command: reset drni troubleshooting history

Old syntax

reset drni troubleshooting history

New syntax

reset m-lag troubleshooting history

Views

User view

Command changes in Track

Modified command: track drni-mad-status

Old syntax

track *track-entry-number* **drni-mad-status**

undo track *track-entry-number*

New syntax

track *track-entry-number* **mlag-mad-status**

undo track *track-entry-number*

Views

System view

Command changes in portal

Modified command: portal drni load-sharing-mode

Old syntax

portal drni load-sharing-mode { **centralized** | **distributed** { **even-ip** | **odd-ip** } }

undo portal drni load-sharing-mode

New syntax

portal m-lag load-sharing-mode { **centralized** | **distributed** { **even-ip** | **odd-ip** } }

undo portal m-lag load-sharing-mode

Views

System view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Modified command: portal drni traffic backup

Old syntax

portal drni traffic backup { **interval** *interval-value* | **threshold** *threshold-value* } *

undo portal drni traffic backup

New syntax

portal m-lag traffic backup { **interval** *interval-value* | **threshold** *threshold-value* } *

undo portal m-lag traffic backup

Views

System view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in Web authentication

Modified command: display web-auth user

Old syntax

display web-auth user [**drni** [**local** | **peer**]] [**interface** *interface-type interface-number* | **slot** *slot-number*]

New syntax

display web-auth user [**m-lag** [**local** | **peer**]] [**interface** *interface-type interface-number* | **slot** *slot-number*]

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in AAA

Modified command: nas-ip (RADIUS scheme view)

Old syntax

nas-ip [**drni** { **local** | **peer** }] { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo nas-ip [**drni** { **local** | **peer** }] [**interface** | **ipv6**]

New syntax

nas-ip [**m-lag** { **local** | **peer** }] { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo nas-ip [**m-lag** { **local** | **peer** }] [**interface** | **ipv6**]

Views

RADIUS scheme view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in 802.1X

Modified command: display dot1x connection

Old syntax

display dot1x connection [**open**] [[**drni** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** } | **slot** *slot-number* | **user-name** *name-string*] | **user-mac** *mac-address*]

New syntax

display dot1x connection [**open**] [[**m-lag** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** } | **slot** *slot-number* | **user-name** *name-string*] | **user-mac** *mac-address*]

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in MAC authentication

Modified command: display mac-authentication connection

Old syntax

display mac-authentication connection [**open**] [[**drni** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } | **slot** *slot-number* | **user-name** *user-name*] | **user-mac** *mac-address*]

New syntax

display mac-authentication connection [**open**] [[**m-lag** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } | **slot** *slot-number* | **user-name** *user-name*] | **user-mac** *mac-address*]

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in port security

Modified command: display port-security access-user

Old syntax

display port-security access-user [**drni** [**local** | **peer**]] [**access-type** { **dot1x** | **mac-auth** | **web-auth** | **static** } | **domain** *domain-name* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } | **slot** *slot-number*] *

New syntax

display port-security access-user [**m-lag** [**local** | **peer**]] [**access-type** { **dot1x** | **mac-auth** | **web-auth** | **static** } | **domain** *domain-name* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** | **url-unavailable-domain** } | **slot** *slot-number*] *

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Modified command: display port-security static-user connection

Old syntax

display port-security static-user connection [[**drni** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** } | **slot**

slot-number | **user-name** *user-name*] | { **ip** | **ipv6** } *ip-address* | **mac** *mac-address*]

New syntax

display port-security static-user connection [[**m-lag** [**local** | **peer**]] [**interface** *interface-type interface-number* | **online-type** { **auth-fail-domain** | **critical-domain** | **preauth-domain** | **success** } | **slot** *slot-number* | **user-name** *user-name*] | { **ip** | **ipv6** } *ip-address* | **mac** *mac-address*]

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Modified command: port-security drni load-sharing-mode

Old syntax

port-security drni load-sharing-mode { **centralized** | **distributed** { **even-mac** | **local** | **odd-mac** } }

undo port-security drni load-sharing-mode

New syntax

port-security m-lag load-sharing-mode { **centralized** | **distributed** { **even-mac** | **local** | **odd-mac** } }

undo port-security m-lag load-sharing-mode

Views

Any view

Change description

The **drni** keyword was changed to the **m-lag** keyword.

Command changes in DHCP

Modified command: display dhcp snooping drni-statistics

Old syntax

display dhcp snooping drni-statistics [**old-version**]

New syntax

display dhcp snooping m-lag-statistics [**old-version**]

Views

Any view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

Modified command: display dhcp snooping drni-status

Old syntax

display dhcp snooping drni-status

New syntax

display dhcp snooping m-lag-status

Views

Any view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

Modified command: reset dhcp snooping drni-statistics

Old syntax

reset dhcp snooping drni-statistics

New syntax

reset dhcp snooping m-lag-statistics

Views

User view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

Command changes in DHCPv6

Modified command: display ipv6 dhcp snooping drni-statistics

Old syntax

display ipv6 dhcp snooping drni-statistics [**old-version**]

New syntax

display ipv6 dhcp snooping m-lag-statistics [**old-version**]

Views

Any view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

Modified command: display ipv6 dhcp snooping drni-status

Old syntax

display ipv6 dhcp snooping drni-status

New syntax

display ipv6 dhcp snooping m-lag-status

Views

Any view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

Modified command: reset ipv6 dhcp snooping drni-statistics

Old syntax

reset ipv6 dhcp snooping drni-statistics

New syntax

reset ipv6 dhcp snooping m-lag-statistics

Views

User view

Change description

The **drni** keyword in this command was changed to the **m-lag** keyword.

ESS 6702

This release has the following changes:

- New feature: Specifying a security enhanced level
- Modified feature: Configuring MAC authentication
- Modified feature: Disabling BGP from flushing all routes to the routing table
- Modified feature: Support for HMAC-SHA-256 OSPF/OSPFv3 authentication mode
- Modified feature: Displaying the hash keys used for link aggregation load sharing
- Modified feature: DRNI IPP configuration
- Modified feature: Configuring kernel thread deadloop detection

New feature: Specifying a security enhanced level

Specifying a security enhanced level

About this task

The security enhanced level for the device can be 1 and 2, and level 2 indicates a higher security level. If the security enhanced level is set to 2, the following rules apply:

- SSL client policies and SSL server policies do not support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.
- SSL client policies and SSL server policies do not support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation cannot be enabled.

You can specify a security enhanced level as needed.

Restrictions and guidelines

After you change the security enhanced level, for services associated with SSL policies, such as HTTP and SSL VPN, you must re-enable these services to update the associated policies.

Procedure

1. Enter system view.
   `system-view`
2. Specify the security enhanced level for the device.
   `security-enhanced level` *`level-value`*
   By default, the security enhanced level is set to 2.

Command reference

Use **`security-enhanced level`** to specify a security enhanced level for the device.

Use **`undo security-enhanced level`** to restore the default.

Syntax

`security-enhanced level` *`level-value`*

`undo security-enhanced level`

Default

The security enhanced level for the device is 2.

Views

System view

Predefined user roles

network-admin

Parameters

level-value: Specifies the security enhanced level, which can be 1 and 2.

Usage guidelines

The security enhanced level for the device can be 1 and 2, and level 2 indicates a higher security level. If the security enhanced level is set to 2, the following rules apply:

- SSL client policies and SSL server policies do not support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.
- SSL client policies and SSL server policies do not support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation cannot be enabled.

You can specify a security enhanced level as needed.

After you change the security enhanced level, for services associated with SSL policies, such as HTTP and SSL VPN, you must re-enable these services to update the associated policies.

Examples

Set the security enhanced level to 2 for the device.

```
<Sysname> system-view
[Sysname] security-enhanced level 2
```

Modified feature: Configuring MAC authentication

Feature change description

As from this version, when local QoS ID settings exist, make sure the local QoS ID settings meet the following requirements:

- The local QoS ID specified by using the **if-match qos-local-id** command is smaller than 3000.
- The local QoS ID specified by using the **remark qos-local-id** command is smaller than 3000.

Command changes

Syntax

mac-authentication

remark qos-local-id [**egress-active**] *local-id-value*

if-match qos-local-id *local-id-value* [**qppb-manipulation**]

Change description

Before modification: MAC authentication does not have configuration conflicts with the **if-match qos-local-id** or **remark qos-local-id** command when MAC authentication users come online.

After modification: When local QoS ID settings exist, make sure the local QoS ID settings meet the following requirements:

- The local QoS ID specified by using the **if-match qos-local-id** command is smaller than 3000.
- The local QoS ID specified by using the **remark qos-local-id** command is smaller than 3000.

Modified feature: Disabling BGP from flushing all routes to the routing table

Feature change description

As from this release, the **routing-table bgp-rib-only** command can disable BGP from flushing all routes to the routing table, including redistributed routes and routes received from peers and peer groups.

Command changes

Modified command: routing-table bgp-rib-only

Old syntax

routing-table bgp-rib-only [**route-policy** *route-policy-name*]

New syntax

routing-table bgp-rib-only [**all**] [**route-policy** *route-policy-name*]

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

Change description

Before modification: The **routing-table bgp-rib-only** command can only disable BGP from flushing routes received from peers and peer groups to the routing table.

After modification: The **routing-table bgp-rib-only** command supports the **all** keyword. This keyword disables BGP from flushing all routes to the routing table, including redistributed routes and routes received from peers and peer groups. If you do not specify this keyword, BGP does not flush the routes received from the specified peer or peer group to the routing table.

Modified feature: Support for HMAC-SHA-256 OSPF/OSPFv3 authentication mode

Feature change description

As from this release, HMAC-SHA-256 OSPF/OSPFv3 authentication mode is supported.

Command changes

Modified command: authentication-mode

Old syntax

For MD5/HMAC-MD5 authentication:

authentication-mode { **hmac-md5** | **md5** } [*key-id* { **cipher** | **plain** } *string*]

undo authentication-mode [{ **hmac-md5** | **md5** } [*key-id*]]

New syntax

For MD5/HMAC-MD5/HMAC-SHA-256 authentication:

authentication-mode { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id* { **cipher** | **plain** } *string*]

undo authentication-mode [{ **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id*]]

Views

OSPF area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPF authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPF authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: ospf authentication-mode

Old syntax

For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **hmac-md5** | **md5** } [*key-id* { **cipher** | **plain** } *string*]

undo ospf authentication-mode [{ **hmac-md5** | **md5** } [*key-id*]]

New syntax

For MD5/HMAC-MD5/HMAC-SHA-256 authentication:

ospf authentication-mode { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id* { **cipher** | **plain** } *string*]

undo ospf authentication-mode [{ **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id*]]

Views

Interface view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPF authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPF authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: vlink-peer

Old syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | [**authentication-none** | { **hmac-md5** | **md5** } [*key-id* { **cipher** | **plain** } *string*] | **keychain** *keychain-name* | **simple** [{ **cipher** | **plain** } *string*]] | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | [**authentication-none** | { **hmac-md5** | **md5** } [*key-id*] | **keychain**] | **retransmit** | **simple** | **trans-delay**] *

New syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | [**authentication-none** | { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id* { **cipher** | **plain** } *string*] | **keychain** *keychain-name* | **simple** [{ **cipher** | **plain** } *string*]] | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | [**authentication-none** | { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id*] | **keychain**] | **retransmit** | **simple** | **trans-delay**] *

Views

OSPF area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPF authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPF authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: authentication-mode

Old syntax

authentication-mode keychain *keychain-name*

undo authentication-mode

New syntax

For HMAC-SHA-256 authentication:

authentication-mode hmac-sha-256 *key-id* { **cipher** | **plain** } *string*

undo authentication-mode

For keychain authentication:

authentication-mode keychain *keychain-name*

undo authentication-mode

Views

OSPFv3 area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPFv3 authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPFv3 authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: ospfv3 authentication-mode

Old syntax

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode [**instance** *instance-id*]

New syntax

For HMAC-SHA-256 authentication:

ospfv3 authentication-mode hmac-sha-256 *key-id* { **cipher** | **plain** } *string* [**instance** *instance-id*]

undo ospfv3 authentication-mode [**instance** *instance-id*]

For keychain authentication:

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode [**instance** *instance-id*]

Views

Interface view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPFv3 authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPFv3 authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: vlink-peer

Old syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **keychain** *keychain-name* | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | **ipsec-profile** | **keychain** | **retransmit** | **trans-delay**] *

New syntax

vlink-peer *router-id* [**dead** *seconds* | **hello** *seconds* | **instance** *instance-id* | **ipsec-profile** *profile-name* | [**hmac-sha-256** *key-id* { **cipher** | **plain** } *string* | **keychain** *keychain-name*] | **retransmit** *seconds* | **trans-delay** *seconds*] *

undo vlink-peer *router-id* [**dead** | **hello** | **ipsec-profile** | [**hmac-sha-256** | **keychain**] | **retransmit** | **trans-delay**] *

Views

OSPFv3 area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPFv3 authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPFv3 authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: sham-link (OSPF area view)

Old syntax

sham-link *source-ip-address destination-ip-address* [**cost** *cost-value* | **dead** *dead-interval* | **hello** *hello-interval* | { **authentication-none** | { **hmac-md5** | **md5** } [*key-id* { **cipher** | **plain** } *string*] | **keychain** *keychain-name* | **retransmit** *retrans-interval* | **simple** [{ **cipher** | **plain** } *string*] } | **trans-delay** *delay* | **ttl-security hops** *hop-count*] *

undo sham-link *source-ip-address destination-ip-address* [**cost** | **dead** | **hello** | { **authentication-none** | { **hmac-md5** | **md5** } [*key-id*] | **keychain** | **simple** } | **retransmit** | **trans-delay** | **ttl-security**] *

New syntax

sham-link *source-ip-address destination-ip-address* [**cost** *cost-value* | **dead** *dead-interval* | **hello** *hello-interval* | { **authentication-none** | { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id* { **cipher** | **plain** } *string*] | **keychain** *keychain-name* | **simple** [{ **cipher** | **plain** } *string*] } | **retransmit** *retrans-interval* | **trans-delay** *delay* | **ttl-security hops** *hop-count*] *

undo sham-link *source-ip-address destination-ip-address* [**cost** | **dead** | **hello** | { **authentication-none** | { **hmac-md5** | **hmac-sha-256** | **md5** } [*key-id*] | **keychain** | **simple** } | **retransmit** | **trans-delay** | **ttl-security**] *

Views

OSPF area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPF authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPF authentication mode by specifying the **hmac-sha-256** keyword.

Modified command: sham-link (OSPFv3 area view)

Old syntax

sham-link *source-ipv6-address destination-ipv6-address* [**cost** *cost-value* | **dead** *dead-interval* | **hello** *hello-interval* | **instance** *instance-id* | **ipsec-profile** *profile-name* | **keychain** *keychain-name* | **retransmit** *retrans-interval* | **trans-delay** *delay*] *

undo sham-link *source-ipv6-address destination-ipv6-address* [**cost** | **dead** | **hello** | **ipsec-profile** | **keychain** | **retransmit** | **trans-delay**] *

New syntax

sham-link *source-ipv6-address destination-ipv6-address* [**cost** *cost-value* | **dead** *dead-interval* | **hello** *hello-interval* | **instance** *instance-id* | **ipsec-profile** *profile-name* | { **hmac-sha-256** *key-id* { **cipher** | **plain** } *string* | **keychain** *keychain-name* } | **retransmit** *retrans-interval* | **trans-delay** *delay*] *

undo sham-link *source-ipv6-address destination-ipv6-address* [**cost** | **dead** | **hello** | **ipsec-profile** | { **hmac-sha-256** | **keychain** } | **retransmit** | **trans-delay**] *

Views

OSPFv3 area view

Change description

Before modification: This command does not support the **hmac-sha-256** keyword. You cannot enable the HMAC-SHA-256 OSPFv3 authentication mode.

After modification: This command supports the **hmac-sha-256** keyword. You can enable the HMAC-SHA-256 OSPFv3 authentication mode by specifying the **hmac-sha-256** keyword.

Modified feature: Displaying the hash keys used for link aggregation load sharing

Feature change description

From this software version on, the device displays the hash keys used for load sharing Layer 2 and Layer 3 traffic over aggregate links.

Command changes

Modified command: display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode [**interface** [{ **bridge-aggregation** | **route-aggregation** | **schannel-bundle** } *interface-number*]]

Views

Any view

Change description

Before modification: The **display link-aggregation load-sharing mode** command does not display load sharing hash keys for Layer 2 or Layer 3 traffic.

```
<Sysname> display link-aggregation load-sharing mode
MAC-in-MAC traffic load-sharing mode:
Outer (default)
Link-aggregation load-sharing algorithm:
5 (default)
Link-aggregation load-sharing offset:
0 (default)
Link-aggregation load-sharing seed:
```

```
0x0 (default)
Tunneled traffic load-sharing mode:
Outer (default)
Link-aggregation load-sharing mode:
  Layer 2 traffic:   packet type-based sharing
  Layer 3 traffic:   packet type-based sharing
```

After modification: The **display link-aggregation load-sharing mode** command displays load sharing hash keys for Layer 2 and Layer 3 traffic.

```
<Sysname> display link-aggregation load-sharing mode
MAC-in-MAC traffic load-sharing mode:
Outer (default)
Link-aggregation load-sharing algorithm:
5 (default)
Link-aggregation load-sharing offset:
0 (default)
Link-aggregation load-sharing seed:
0x0 (default)
Tunneled traffic load-sharing mode:
Outer (default)
Link-aggregation load-sharing mode:
  Layer 2 traffic:   destination-mac address, source-mac address
                     ethernet-type
  Layer 3 traffic:   destination-ip address, source-ip address
                     destination-port, source-port
                     ip-protocol
```

Modified feature: DRNI IPP configuration

Feature change description

Before modification: The link type and VLAN assignment settings are not automatically issued to an aggregate interface after you configure it as the IPP. You can assign the IPP role to an aggregate interface before you assign member ports to the corresponding aggregation group.

After modification: The link type and VLAN assignment settings are automatically issued to an aggregate interface after you configure it as the IPP. Before you assign the IPP role to an aggregate interface, you must assign member ports to the corresponding aggregation group.

```
[Sysname-Bridge-Aggregation11] display this
#
interface Bridge-Aggregation11
port link-type trunk
port trunk permit vlan all
port drni intra-portal-port 1
#
return
```

Command changes

None.

Modified feature: Configuring kernel thread deadloop detection

Feature change description

As from this release, upon detecting a thread that occupies the CPU for a specific interval, the device determines that a deadloop has occurred, logs the event, and reboots to remove the deadloop.

Command changes

Modified command: monitor kernel deadloop enable

Syntax

monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number* [**core** *core-number*&<1-64>]]]

undo monitor kernel deadloop enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

System view

Change description

Before modification: This feature enables the device to detect deadloops. If a thread occupies the CPU for a specific interval, the device determines that a deadloop has occurred and logs the event.

After modification: This feature enables the device to detect deadloops. If a thread occupies the CPU for a specific interval, the device determines that a deadloop has occurred, logs the event, and reboots to remove the deadloop.