



**Hewlett Packard**  
Enterprise

# HPE 5950-CMW710-R6301P02 Release Notes

# Contents

Introduction.....	1
Version information.....	1
Version number .....	1
Version history .....	1
Hardware and software compatibility matrix .....	8
ISSU compatibility list .....	10
Upgrade restrictions and guidelines .....	10
Hardware feature updates.....	11
R6301P02 .....	11
R6301P01 .....	11
R6301 .....	11
F6207 .....	11
F6206 .....	11
R6205P03 .....	11
F6205P02.....	11
F6205 .....	11
F6203 .....	11
F6202 .....	12
R6125.....	12
R6123.....	12
R6106P01 .....	13
R6106.....	13
R6105.....	13
Software feature and command updates .....	13
MIB updates.....	13
Operation changes .....	15
Operation changes in F6301P02.....	15
Operation changes in F6301P01.....	15
Operation changes in R6301 .....	15
Operation changes in F6207 .....	16
Operation changes in F6206 .....	16
Operation changes in R6205P03 .....	17
Operation changes in F6205P02.....	17
Operation changes in F6205 .....	18
Operation changes in F6203 .....	18
Operation changes in F6202 .....	18

Operation changes in R6125.....	19
Operation changes in R6123.....	19
Operation changes in R6106P01 .....	19
Operation changes in R6106.....	19
Operation changes in R6105.....	19
<b>Restrictions and cautions .....</b>	<b>20</b>
<b>Open problems and workarounds .....</b>	<b>20</b>
<b>List of resolved problems .....</b>	<b>20</b>
Resolved problems in R6301P02 .....	20
Resolved problems in R6301P01 .....	21
Resolved problems in R6301.....	21
Resolved problems in F6207 .....	28
Resolved problems in F6206 .....	30
Resolved problems in R6205P03 .....	32
Resolved problems in F6205P02 .....	33
Resolved problems in F6205 .....	34
Resolved problems in F6203 .....	35
Resolved problems in F6202 .....	36
Resolved problems in R6125.....	37
Resolved problems in R6123.....	38
Resolved problems in R6106P01 .....	39
Resolved problems in R6106.....	40
Resolved problems in R6105.....	40
<b>Support and other resources.....</b>	<b>40</b>
Accessing Hewlett Packard Enterprise Support.....	40
Documents .....	41
Related documents.....	41
Documentation feedback .....	41
<b>Appendix A Feature list .....</b>	<b>42</b>
Hardware features.....	42
Software features.....	44
<b>Appendix B Upgrading software .....</b>	<b>48</b>
System software file types .....	48
System startup process .....	48
Upgrade methods .....	49
Upgrading from the CLI .....	50
Preparing for the upgrade .....	50
Downloading software to the master switch .....	51

Upgrading the software images .....	53
Installing a patch package .....	55
Upgrading from the Boot menu .....	56
Prerequisites .....	56
Accessing the Boot menu .....	57
Accessing the basic Boot menu .....	58
Accessing the extended Boot menu .....	59
Using TFTP to upgrade software images through the management Ethernet port .....	60
Using FTP to upgrade software through the management Ethernet port .....	62
Using XMODEM to upgrade software through the console port .....	64
Using TFTP to upgrade Boot ROM through the management Ethernet port .....	68
Using FTP to upgrade Boot ROM through the management Ethernet port .....	69
Using XMODEM to upgrade Boot ROM through the console port .....	71
Managing files from the Boot menu .....	75
Displaying all files .....	75
Deleting files .....	76
Changing the attribute of software images .....	76
Handling software upgrade failures .....	78

# List of tables

Table 1 Version history .....	1
Table 2 Hardware and software compatibility matrix .....	8
Table 3 ISSU compatibility list .....	10
Table 4 MIB updates.....	13
Table 5 5950 series hardware features.....	42
Table 6 Software features of the MSR 20/MSR 30/MSR 50 series.....	44
Table 7 Shortcut keys .....	57
Table 8 Basic Boot ROM menu options .....	58
Table 9 BASIC ASSISTANT menu options.....	59
Table 10 Extended Boot ROM menu options.....	60
Table 11 EXTENDED ASSISTANT menu options .....	60
Table 12 TFTP parameter description .....	61
Table 13 FTP parameter description.....	63
Table 14 TFTP parameter description .....	69
Table 15 FTP parameter description.....	70

# Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version R6301P02. Before you use this version on 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 5950-CMW710-R6301P02 Release Notes (Software Feature Changes) and the documents listed in "[Related documents](#)."

## Version information

### Version number

HPE Comware Software, Version 7.1.070, Release 6301P02

Note: You can see the version number with the **display version** command in any view. Please see Note ①.

### Version history

#### ① 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
5950-CMW710-R6301P02	5950-CMW710-R6301P01	2023-04-28	Release version	<ul style="list-style-type: none"><li>MIB updates.</li></ul>
5950-CMW710-R6301P01	5950-CMW710-R6301	2022-12-31	Release version	<ul style="list-style-type: none"><li>Fixed bugs.</li></ul>
5950-CMW710-R6301	5950-CMW710-F6207	2019-06-12	Release version	<p>New feature includes:</p> <ul style="list-style-type: none"><li>New features: Fundamentals features</li><li>New features: Virtual technologies features</li><li>New features: Layer 2-LAN switching features</li><li>New features: Layer 3-IP services features</li><li>New features: Layer 3-IP routing features</li><li>New features: IP multicast features</li><li>New features: MPLS features</li><li>New features: ACL and QoS features</li><li>New features: Security</li></ul>

Version number	Last version	Release date	Release type	Remarks
				<p>features</p> <ul style="list-style-type: none"> <li>• New features: High availability features</li> <li>• New features: Network management and monitoring features</li> <li>• New features: FC and FCoE features</li> <li>• New features: OpenFlow features</li> <li>• New features: VXLAN features</li> <li>• New features: EVPN features</li> <li>• New feature: Specifying the NTP time-offset thresholds for log and trap outputs</li> <li>• New feature: Specifying the SNTP time-offset thresholds for log and trap outputs</li> </ul> <p>Modified features includes:</p> <ul style="list-style-type: none"> <li>• Modified feature: ISSU by using issu commands</li> <li>• Modified feature: Automatic configuration</li> <li>• Modified feature: Setting the timestamp format for logs sent to log hosts</li> <li>• Modified feature: Configuring an interface event for a CLI-defined EAA monitor policy</li> <li>• Modified feature: Configuring an EAA monitor policy by using Tcl</li> <li>• Modified feature: Displaying the operating status and information of an interface</li> <li>• Modified feature: Displaying PFC information of all interfaces</li> <li>• Modified feature: Link state change suppression on an interface</li> <li>• Modified feature: MAC-to-VLAN entries</li> <li>• Modified feature: Collision handling process of LACP MAD and BFD MAD</li> <li>• Modified feature: Collision handling process of ND MAD</li> <li>• Modified feature: Displaying global link aggregation load sharing</li> </ul>

Version number	Last version	Release date	Release type	Remarks
				<p>modes</p> <ul style="list-style-type: none"> <li>• Modified feature: Configuring a link aggregation load sharing hash seed</li> <li>• Modified feature: Displaying detailed information about the IPP and DR interfaces of DRNI</li> <li>• Modified feature: Configuring the advertisable TLVs for LLDP</li> <li>• Modified feature: Setting the aging timer for dynamic ARP entries</li> <li>• Modified feature: ARP snooping</li> <li>• Modified feature: Specifying DHCP servers for a DHCP relay address pool</li> <li>• Modified feature: Displaying DHCP snooping and DHCPv6 snooping trusted ports</li> <li>• Modified feature: Displaying DHCP address pool information</li> <li>• Modified feature: Displaying DHCPv6 address pool information</li> <li>• Modified feature: Enabling recording DHCPv6 snooping address entries in VLAN view</li> <li>• Modified feature: Setting the aging timer for ND entries in stale state</li> <li>• Modified feature: Displaying member interfaces shut down by Monitor Link</li> <li>• Modified feature: Displaying DLDP configuration</li> <li>• Modified feature: Configuring routing policy-based recursive lookup</li> <li>• Modified feature: Associating Track with the output interface for a static route</li> <li>• Modified feature: Configuring OSPF area authentication</li> <li>• Modified feature: Configuring OSPF</li> </ul>



Version number	Last version	Release date	Release type	Remarks
				<p>interface authentication</p> <ul style="list-style-type: none"> <li>• Modified feature: Configuring a virtual link</li> <li>• Modified feature: Setting the number of OSPF logs</li> <li>• Modified feature: Displaying IS-IS LSP log information</li> <li>• Modified feature: Clearing IS-IS LSP log information</li> <li>• Modified feature: Specifying a label allocation mode</li> <li>• Modified feature: Displaying BGP peer or peer group information</li> <li>• Modified feature: Displaying AS path information for BGP routes</li> <li>• Modified feature: Displaying RPF information for an IPv6 multicast source</li> <li>• Modified feature: Displaying statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping</li> <li>• Modified feature: Displaying statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping</li> <li>• Modified feature: Enabling a VPN instance to replicate routes from the public network or other VPN instances</li> <li>• Modified feature: Specifying outgoing labels for a static SRLSP</li> <li>• Modified feature: Creating an ACL</li> <li>• Modified feature: Referencing an ACL in QoS or packet filtering</li> <li>• Modified feature: Enabling hardware-count for the packet filtering default action</li> <li>• Modified feature: Configuring drop-level-based parameters for a queue in a WRED table</li> <li>• Modified feature: Configuring binding</li> </ul>

Version number	Last version	Release date	Release type	Remarks
				<ul style="list-style-type: none"> <li>attributes for a local user</li> <li>Modified feature: Password handling when global password control is enabled</li> <li>Modified feature: Setting the quiet timer for RADIUS servers</li> <li>Modified feature: Configuring MAC-based MAC authentication user accounts</li> <li>Modified feature: MAC authentication VLAN mode</li> <li>Modified feature: Port security MAC move</li> <li>Modified feature: Web authentication support for HTTPS redirection</li> <li>Modified feature: RSA key modulus length</li> <li>Modified feature: RSA key modulus length used for certification request in a PKI domain</li> <li>Modified feature: Displaying IPv4SG bindings</li> <li>Modified feature: Displaying IPv6SG bindings</li> <li>Modified feature: Displaying the MFF configuration for a VLAN</li> <li>Modified feature: Associating Track with application modules</li> <li>Modified feature: Specifying the length of ICMP echo requests sent by an IPv4 or IPv6 ping operation</li> <li>Modified feature: Removing a TCP or UDP listening service for a VPN instance</li> <li>Modified feature: Specifying the source IP address for NTP messages</li> <li>Modified feature: Creating a sampler</li> <li>Modified feature: sFlow counter sampling</li> <li>Modified feature: sFlow flow sampling</li> <li>Modified feature: Configuring a backup PW</li> </ul>

Version number	Last version	Release date	Release type	Remarks
				for a cross-connect <ul style="list-style-type: none"> <li>Modified feature: Configuring a backup PW for a VSI</li> <li>Modified feature: Change of the bandwidth limit value range for VSIs</li> <li>Modified feature: Value range change for the broadcast, multicast, or unknown unicast restraint bandwidth of VSIs</li> <li>Modified feature: Frame match criteria of VXLAN Ethernet service instances</li> <li>Modified feature: Displaying EVPN routing table information</li> <li>Modified feature: NETCONF logging</li> <li>Modified feature: Specifying the role of the device in the VCF fabric</li> </ul> Fixed bugs.
5950-CMW710-F6207	5950-CMW710-F6206	2019-01-28	Feature version	This version fixed bugs and introduced feature changes. New features include: <ul style="list-style-type: none"> <li>Changing the next hop address of VPNv4 routes to a VPN address</li> </ul> There are also modified features.
5950-CMW710-F6206	5950-CMW710-R6205P03	2018-08-15	Feature version	This version fixed bugs and introduced feature changes. New features include: <ul style="list-style-type: none"> <li>Setting fan tray serial numbers</li> <li>Simple multichassis link aggregation (S-MLAG)</li> <li>Configuring PFC deadlock detection</li> </ul> There are also modified features.
5950-CMW710-R6205P03	5950-CMW710-F6205P02	2017-11-13	Feature version	This version fixed bugs and introduced feature changes. New features include: <ul style="list-style-type: none"> <li>Enabling STP dispute guard</li> <li>Enabling DNS spoofing</li> <li>Enabling symmetric load sharing</li> </ul> There are also modified

Version number	Last version	Release date	Release type	Remarks
				features.
5950-CMW710-F6205P02	5950-CMW710-F6205	2017-10-30	Feature version	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> <li>• Setting PFC thresholds</li> <li>• Local-MAC address learning</li> <li>• Conversational learning for remote MAC address entries</li> </ul> <p>Removed features include:</p> <ul style="list-style-type: none"> <li>• Ignoring port speed in setting the aggregation states of member ports</li> <li>• PBB</li> <li>• SPBM</li> </ul> <p>There are also modified features.</p>
5950-CMW710-F6205	5950-CMW710-F6203	2017-6-28	Feature version	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> <li>• One-step ISSU</li> <li>• Specifying ignored packet fields for the default link-aggregation load sharing</li> <li>• Static SR over MPLS</li> </ul> <p>There are also modified features.</p>
5950-CMW710-F6203	5950-CMW710-F6202	2017-4-27	Feature version	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> <li>• DRNI</li> </ul>
5950-CMW710-F6202	5950-CMW710-R6125	2017-3-28	Feature version	<p>This version fixed bugs and introduced feature changes.</p> <p>New features include:</p> <ul style="list-style-type: none"> <li>• FC and FCoE</li> <li>• MACsec</li> <li>• EEE</li> <li>• PBB</li> <li>• MPLS L2VPN</li> <li>• VPLS</li> <li>• SPBM</li> <li>• ERPS</li> <li>• FNA(HPE FlexFabric Network Analytics)</li> <li>• DCBX</li> </ul> <p>There are also modified features.</p>
5950-CMW710-R6	5950-CMW710-R	2017-1-13	Release	<ul style="list-style-type: none"> <li>• Fixed bugs.</li> </ul>

Version number	Last version	Release date	Release type	Remarks
125	6123		version	<ul style="list-style-type: none"> <li>Modified features.</li> </ul>
5950-CMW710-R6 123	5950-CMW710-R 6106P01	2016-9-30	Release version	Added feature and new devices.
5950-CMW710-R6 106P01	5950-CMW710-R 6106	2016-9-11	Release version	Added feature: <ul style="list-style-type: none"> <li>New feature: Load balancing among BGP routes with different AS_PATH attributes of the same length</li> </ul>
5950-CMW710-R6 106	5950-CMW710-R 6105	2016-5-31	Release version	Fixed bugs.
5950-CMW710-R6 105	First release	2016-4-11	Release version	None

## Hardware and software compatibility matrix



### CAUTION:

To avoid an upgrade failure, use [Table 2](#) to verify the hardware and software compatibility before performing an upgrade.

**Table 2 Hardware and software compatibility matrix**

Item	Specifications
Product family	HPE 5950 Series
Hardware platform	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A HPE FlexFabric 5950 4-slot Switch JH404A
Memory	4GB
Flash	1GB
Boot ROM version	Version 106 or higher (Note: Perform the command <b>display version</b> command in any view to view the version information. Please see Note②)
Host software	5950-CMW710-R6301P02.ipe

Item	Specifications
iMC version	iMC BIMS 7.3(E0501) iMC EAD 7.3 (E0502) iMC EIA 7.3(E0503) iMC TAM 7.3 (E0503) iMC UAM 7.3 (E0503) iMC MVM 7.3 (E0501) iMC NTA 7.3 (E0502) iMC PLAT 7.3 (E0605) iMC QoSM 7.3 (E0502) iMC-RAM 7.3(E0501) iMC UBA 7.3 (E0502) iMC VFM 7.3 (E0502)
iMC version for FNA	iNode PC 7.3(E0504)
iNode version	None
Web version	None
OAA version	None

To display version information for the system software and Boot ROM of 5950:

```
<HPE> display version
```

```
HPE Comware Software, Version 7.1.070, Release 6301P02 ----- Note①
```

```
Copyright (c) 2010-2023 Hewlett Packard Enterprise Development LP
```

```
HPE FF 5950 32Q28 Switch uptime is 0 weeks, 0 days, 1 hour, 16 minutes
```

```
Last reboot reason : Auto Update reboot
```

```
Boot image: flash:/s6820-cmw710-boot-r6301p02.bin
```

```
Boot image version: 7.1.070, Release 6301P02
```

```
Compiled Mar 22 2023 11:00:00
```

```
System image: flash:/s6820-cmw710-system-r6301p02.bin
```

```
System image version: 7.1.070, Release 6301P02
```

```
Compiled Mar 22 2023 11:00:00
```

```
Slot 1:
```

```
Uptime is 0 weeks,2 days,3 hours,5 minutes
```

```
FF 5950 32Q28 Switch with 2 Processor
```

```
BOARD TYPE: FF 5950 32Q28 Switch
```

```
DRAM: 3584M bytes
```

```
FLASH: 1024M bytes
```

```
PCB 1 Version: VER.B
```

```
PCB 2 Version: VER.B
```

```
FPGA Version: NONE
```

```
Bootrom Version: 106
```

```
----- Note②
```

```

CPLD 1 Version:    001
CPLD 2 Version:    001
Release Version:    HPE FF 5950 32Q28 Switch-6301P02
Patch Version:      None
Reboot Cause:       UserReboot
[SubSlot 0] 32QSFP28 + 2SFP PLUS

```

## ISSU compatibility list

**Table 3 ISSU compatibility list**

Current version	Earlier version	ISSU compatibility
5950-CMW710-R6301P02	5950-CMW710-R6301P01	No
	5950-CMW710-R6301	No
	5950-CMW710-F6207	Yes
	5950-CMW710-F6206	Yes
	5950-CMW710-R6205P03	Yes
	5950-CMW710-F6205P02	Yes
	5950-CMW710-F6205	Yes
	5950-CMW710-F6203	Yes
	5950-CMW710-F6202	Yes
	5950-CMW710-R6125	Yes
	5950-CMW710-R6123	No
	5950-CMW710-R6106P01	No
	5950-CMW710-R6106	No
	5950-CMW710-R6105	No

## Upgrade 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 documents](#)") available on the HPE website for more information about feature configuration and commands.

Because Release 6106 and later versions support new signatures, the software cannot be downgraded to Release 6105 after it is upgraded to Release 6106 or later.

When the software is upgraded to or from version F6202/F6203, the **port media-type** configuration might change. If the port media type configuration changes, you must configure the port media type again as needed. This command is available only on the lowest-numbered eight 25-GE interfaces and highest-numbered eight 25-GE interfaces on the HPE FlexFabric 5950 48SFP28 8QSFP28 Switch (JH402A) and the 25-GE interfaces on the LSWM124TG2H interface module of the HPE FlexFabric 5950 4-slot Switch (JH404A).

If the device is configured with FlexFabric Network Analytics (FNA), do not use ISSU to upgrade the software to version F6205.

When the software is upgraded to or from version F6205 by using ISSU, IRF split might occur to cause software upgrade failure. As a best practice, do not use ISSU to upgrade the software to version F6205 or upgrade the software from version F6205 to another version.

## Hardware feature updates

### R6301P02

None.

### R6301P01

None.

### R6301

None.

### F6207

The following transceiver modules are supported:

- QSFP-100G-ER4L-WDM1300

### F6206

The following transceiver modules are supported:

- HPE X150 100G QSFP28 LC SWDM4 100m MM Transceiver(JH419A)

### R6205P03

None.

### F6205P02

The HPE FlexFabric 5950 4-slot Switch supports the new subcard LSWM18CQMSEC (JH957A).

### F6205

None.

### F6203

None.



# F6202

The following transceiver modules are supported:

- HPE X190 8G/4G/2G SFP+ LC Short Wave Transceiver JG879A
- HPE X190 8G/4G/2G SFP+ LC Long Wave Transceiver JG880A

The Mellanox 655874-B21 QSFP+ to SFP+ adapter is supported. When a 100G QSFP28 interface or 40G QSFP+ interface has this adapter installed, the interface is compatible with a 10G SFP+ transceiver module. LSWM116Q Interface Card (JH405A) does not support this adapter.

# R6125

None.

# R6123

The following devices are supported:

- HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A
- HPE FlexFabric 5950 4-slot Switch JH404A

The following expansion cards are supported:

- LSWM18CQ
- LSWM116Q
- LSWM124TG2H
- LSWM124XGT2Q
- LSWM124XG2QFC
- LSWM18QC
- LSWM124XG2Q
- LSWM124XG2QL

The following transceiver modules are supported:

- HPE X150 100G QSFP28 LC LR4 10km SM Transceiver(JL275A)
- HPE X240 100G QSFP28 to QSFP28 5m Direct Attach Copper Cable(JL273A)
- HPE X2A0 100G QSFP28 to QSFP28 7m Active Optical Cable(JL276A)
- HPE X2A0 100G QSFP28 to QSFP28 10m Active Optical Cable(JL277A)
- HPE X2A0 100G QSFP28 to QSFP28 20m Active Optical Cable(JL278A)
- HPE X240 QSFP28 4xSFP28 1m DAC Cable(JL282A)
- HPE X240 QSFP28 4xSFP28 3m DAC Cable(JL283A)
- HPE X2A0 40G QSFP+ to QSFP+ 7m Active Optical Cable(JL287A)
- HPE X2A0 40G QSFP+ to QSFP+ 10m Active Optical Cable(JL288A)
- HPE X2A0 40G QSFP+ to QSFP+ 20m Active Optical Cable(JL289A)
- HPE X190 25G SFP28 LC SR 100m MM XCVR(JL293A)
- HPE X240 25G SFP28 to SFP28 1m DAC(JL294A)
- HPE X240 25G SFP28 to SFP28 3m DAC(JL295A)

# R6106P01

None.

# R6106

The following transceiver modules are supported:

- HPE X2A0 10G SFP+ to SFP+ 7m Active Optical Cable (JL290A)
- HPE X2A0 10G SFP+ to SFP+ 10m Active Optical Cable(JL291A)
- HPE X2A0 10G SFP+ to SFP+ 20m Active Optical Cable(JL292A)

# R6105

First release.

## Software feature and command updates

For more information about the software feature and command update history, see *HPE 5950-CMW710-R6301P02 Release Notes (Software Feature Changes)*.

## MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
<b>5950-CMW710-R6301P02</b>			
New	hh3c-arp-suppression.mib	HH3C-ARP-SUPPRESSION-MIB	Added hh3cARPSuppressionChassis hh3cARPSuppressionSlot hh3cARPSuppressionVsiName hh3cARPSuppressionIpAddress hh3cARPSuppressionMacAddress hh3cARPSuppressionLinkID hh3cARPSuppressionAging
Modified	None	None	None
<b>5950-CMW710-R6301P01</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-R6301</b>			
New	hh3c-stack.mib	HH3C-STACK-MIB	Added hh3cStackTrapObjects

Item	MIB file	Module	Description
Modified	sflow.mib hh3c-bgp-evpn-mib.mib	SFLOW-MIB HH3C-BGP-EV PN-MIB	Modified sFlowCplInstance sFlowFsInstance hh3cBgpEvpnPAtrAddrPrefix hh3cBgpEvpnPAtrPeer
<b>5950-CMW710-F6207</b>			
New	HH3C-BGP-EVPN-MIB.docx	None	None
Modified	HH3C-TRANSCIVER-INFO-MIB.doc x	hh3cTransceiver InfoTable	Added: hh3cTransceiverPartNumber hh3cTransceiverProductCode
<b>5950-CMW710-F6206</b>			
New	None	None	None
Modified	HH3C-IF-EXT-MIB.docx	hh3clfTable	Added: hh3clfFwdErrDiscards
<b>5950-CMW710-R6205P03</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-F6205P02</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-F6205</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-F6203</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-F6202</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-R6125</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-R6123</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-R6106P01</b>			
New	None	None	None

Item	MIB file	Module	Description
Modified	None	None	None
<b>5950-CMW710-R6106</b>			
New	None	None	None
Modified	None	None	None
<b>5950-CMW710-R6105</b>			
New	First release	First release	First release
Modified	First release	First release	First release

## Operation changes

### Operation changes in F6301P02

None.

### Operation changes in F6301P01

None.

### Operation changes in R6301

- [201810100437]Added support for using existent and nonexistent policies to filter the BGP routes to be advertised to a peer or peer group.
- [201710190032]Added support for MACsec 256-bit encryption to the LSWM18CQMSEC(JH957A) interface module.  
Before modification: The LSWM18CQMSEC(JH957A) interface module only supports the default MACsec 128-bit encryption.  
After modification: The **macsec cipher-suite gcm-aes-256** and **macsec cipher-suite gcm-aes-128** commands were added. You can use these commands to enable 256-bit encryption and 128-bit encryption on the LSWM18CQMSEC(JH957A) interface module.
- [201811260646]Removed the **I - Invalid** value from the **Flags** field in the output from the **display evpn route nd** command.
- [201708150654]Added DHCP support for OVSDB.
- [201809260394]Added the DRNI MIB.
- [201711140340]Added the EVPN 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.

- [201804270716]Added NETCONF support for reading packet statistics about VSI interfaces used for EVPN or VXLAN Layer 3 forwarding.
- [201904090672]Added support for inbound and outbound rate limiting for Layer 3 subinterfaces.

## Operation changes in F6207

None.

## Operation changes in F6206

- The default maximum size of a PIM and IPv6 PIM join or prune message  
The default maximum size of a PIM and IPv6 PIM join or prune message was changed from 8100 bytes to 1200 bytes. For more information, see *HPE 5950-CMW710-F6206 Release Notes (Software Feature Changes)*.
- VLAN-based VXLAN assignment  
Before modification: If you enable VLAN-based VXLAN assignment and map a VLAN to a VXLAN, the device automatically performs the following operations:
  - Creates an Ethernet service instance that uses the VLAN ID as its instance ID on each interface in the VLAN. The matching outer VLAN ID of the Ethernet service instances is the VLAN ID.
  - Maps the Ethernet service instances to the VSI of the VXLAN.
 After modification:
  - If you enable VLAN-based VXLAN assignment and map a VLAN to a VXLAN, the device automatically performs the following operations:
    - Creates an Ethernet service instance that uses the VLAN ID as its instance ID on each interface in the VLAN.
    - Maps the Ethernet service instances to the VSI of the VXLAN.
  - On an interface, the frame match criterion of the Ethernet service instance is set as follows:
    - If the VLAN ID is the PVID of the interface, the Ethernet service instance matches untagged frames.
    - If the VLAN ID is not the PVID of the interface, the Ethernet service instance matches frames tagged with an outer VLAN ID that is same as that VLAN ID.
- Modify the number of VRRP groups that a device can support to 1024.  
Before modification: A device supports a maximum of 256 VRRP groups.  
After modification: A device supports a maximum of 1024 VRRP groups.
- Creating an ACL  
This software version allows you to specify both a name and a number when creating an ACL. For more information, see *HPE 5950-CMW710-F6206 Release Notes (Software Feature Changes)*
- DRNI configuration consistency check  
VLAN information was added to DRNI configuration consistency check. For more information, see *HPE 5950-CMW710-F6206 Release Notes (Software Feature Changes)*.
- Assigning IP addresses to management Ethernet interfaces  
Before modification: The IP addresses assigned to the management Ethernet interfaces of all IRF member devices must be in the same subnet.  
After modification: The IP addresses must be in the same subnet if you assign them through the same management Ethernet interface of the master device. The IP addresses must be in

different subnets if you assign them through different management Ethernet interfaces of the master device.

- Displaying recommended ISSU methods

This release deleted support for displaying version compatibility information. For more information, see *HPE 5950-CMW710-F6206 Release Notes (Software Feature Changes)*. To identify whether the software versions support ISSU compatible upgrade, see ISSU compatibility list in the release notes.

## Operation changes in R6205P03

None.

## Operation changes in F6205P02

- Modified interface QoS policy application settings

Before modification: You can apply only one QoS policy to each direction of an interface, and only one traffic behavior action can be performed on traffic matching a traffic class.

After modification: You can apply a maximum of three QoS policies of different types to the same direction of an interface: one generic, one accounting-type, and one marking-type. For more information, see *HPE 5950-CMW710-F6205P02 Release Notes (Software Feature Changes)*.

- ARP MAD collision handling process

Before modification: ARP MAD uses the following process to handle a multi-active collision:

- Compares the member IDs of the masters in the split IRF fabrics.
- Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

After modification: ARP MAD uses the following process to handle a multi-active collision:

- Compares the forwarding performance of the chips in each split fabric.
- Sets all fabrics to the Recovery state except the one that has the best chip forwarding performance.
- Compares the member IDs of the masters if all IRF fabrics have the same chip forwarding performance.
- Sets all fabrics to the Recovery state except the one that has the lowest numbered master.

- DRNI and EVPN distributed relay

The **distributed-relay** keyword in DRNI commands and EVPN distributed relay commands were changed to **drni**. For more information, see *HPE 5950-CMW710-F6205P02 Release Notes (Software Feature Changes)*.

- Multicast VPN

MD view was changed to MVPN view and the **multicast-domain** keyword in commands was changed to **multicast-vpn**. For more information, see *HPE 5950-CMW710-F6205P02 Release Notes (Software Feature Changes)*.

- Configuration rollback by using NETCONF

Suppression for the <edit-config> operation during a configuration rollback was added. To allow the <edit-config> operation to be performed during a configuration rollback, you must perform an <action> operation to change the value of the **DisableEditConfigWhenRollback** attribute to **false**. For more information, see *HPE 5950-CMW710-F6205P02 Release Notes (Software Feature Changes)*.

## Operation changes in F6205

- Configuring the FlexFabric Network Analytics (FNA) feature  
This release added support for configuring the FNA feature on an IRF fabric.
- Monitoring CPU usage  
The minor alarm threshold, severe alarm threshold, and recovery threshold were added to monitor CPU usage in finer granularity. For more information, see *HPE 5950-CMW710-F6205 Release Notes (Software Feature Changes)*.
- Configuring IRF bridge MAC persistence  
The MAC address persistent time changed from 10 minutes to 12 minutes for the **irf mac-address persistent timer** command.

## Operation changes in F6203

None.

## Operation changes in F6202

- Support of 10-GE and 25-GE interfaces for the 1Gbps speed  
Before modification: 10-GE and 25-GE interfaces on HPE FlexFabric 5950 48SFP28 8QSFP28 Switch and HPE FlexFabric 5950 4-slot Switch do not support the 1Gbps speed or transceiver module.  
After modification: 10-GE and 25-GE interfaces on HPE FlexFabric 5950 48SFP28 8QSFP28 Switch and HPE FlexFabric 5950 4-slot Switch support the 1Gbps speed or transceiver module.
- Excluding a service interface from the IRF MAD shutdown action by the system  
When the IRF fabric transits to the Recovery state, the system automatically excludes the following service interfaces from being shut down:  
Before modification:
  - IRF physical interfaces.
  - Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.After modification:
  - IRF physical interfaces.
  - Interfaces used for BFD MAD.
  - Member interfaces of an aggregate interface if the aggregate interface is excluded from being shut down.
- Aging time for ARP entries in the output of the display arp command  
Before modification: The command displays the ARP entry aging time in minutes.  
After modification: The command displays the ARP entry aging time in seconds.
- Value range for port security's limit on the number of secure MAC addresses  
The value range for the *max-count* argument of the **port-security max-mac-count max-count [ vlan [ vlan-id-list ] ]** command changed.  
Before modification: The value range for the *max-count* argument is 1 to 4294967295.  
After modification: The value range for the *max-count* argument is 1 to 2147483647.
- Enabling a BGP instance

Support for session multithreading was removed. You can create the same public IPv4 unicast address family on different BGP instances. For more information, see *HPE 5950-CMW710-F6202 Release Notes (Software Feature Changes)*.

- Specifying a RabbitMQ server

In this software version, you can specify the port number through which the device communicates with a RabbitMQ server when you specify the RabbitMQ server. You can specify the MPLS L3VPN instance to which a RabbitMQ server belongs when you remove the RabbitMQ server. For more information, see *HPE 5950-CMW710-F6202 Release Notes (Software Feature Changes)*.

- IChanged the default load sharing mode for IP tunneled traffic for the ip load-sharing mode command

Before modification: If you do not specify the **tunnel { all | inner | outer }** parameters in the ip load-sharing mode command, IP tunneled traffic is distributed based on the outer IP header.

After modification: If you do not specify the **tunnel { all | inner | outer }** parameters in the ip load-sharing mode command, IP tunneled traffic is distributed based on the inner IP header.

## Operation changes in R6125

- Number of subinterfaces supported

Before modification, you can create 500 Layer 3 Ethernet subinterfaces and Layer 3 aggregate subinterfaces in total.

After modification, you can create 1024 Layer 3 Ethernet subinterfaces and Layer 3 aggregate subinterfaces in total.

- CL72 negotiation

Before modification, CL72 negotiation is enabled by default.

After modification, CL72 negotiation is disabled by default.

## Operation changes in R6123

- Configuring IRF bridge MAC persistence

The MAC address persistent time changed from 6 minutes to 10 minutes for the **irf mac-address persistent timer** command.

## Operation changes in R6106P01

None.

## Operation changes in R6106

None.

## Operation changes in R6105

First release.



# Restrictions and cautions

To connect an interface on the LSWM124XG2QL(JH180A) interface module or a 25-GE interface with a GE transceiver module to another device, you must perform the following tasks on the interface:

- Set the interface speed to 1000 Mbps by using the **speed 1000** command.
- Configure the interface to operate in full duplex mode by using the **duplex full** command.

When multiple queues on one interface or multiple interfaces exceed the buffer usage threshold in FNA at the same time, alarms are not reported for some queues, and the corresponding queue monitor graphs are incorrect.

Multicast packets cannot trigger FNA alarms on the following interfaces:

- 10-GE interfaces on the HPE FlexFabric 5950 32QSFP28 Switch (JH321A) and HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch (JH322A).
- GE interfaces on the HPE FlexFabric 5950 48SFP28 8QSFP28 Switch (JH402A) and HPE FlexFabric 5950 4-slot Switch (JH404A).

# Open problems and workarounds

## 201612230336

- Symptom: After a tunnel interface comes up, the interface cannot decapsulate and forward packets received from VTEPs.
- Condition: This symptom occurs if multiple tunnels exist and the source IP address of one tunnel is the global source IP address. Then, the tunnel that is not configured with a source IP address can come up, but the tunnel interface cannot decapsulate and forward packets received from VTEPs.
- Workaround: Make sure the source IP address configured for a tunnel is different from the global source IP address.

## 201808170465

- Symptom: NetStream is unavailable on a shutdown GigabitEthernet interface on the rear panel.
- Condition: This symptom might occur if NetStream is enabled on a shutdown GigabitEthernet interface on the rear panel.
- Workaround: Bring up the GigabitEthernet interface.

## 201901150116

- Symptom: In a VPLS network, if RSVP is used to distribute labels for MPLS TE tunnels, an MPLS TE tunnel cannot switch traffic from the failed primary path to the backup path.
- Condition: This symptom might occur if RSVP is used to distribute labels for MPLS TE tunnels in a VPLS network.
- Workaround: None.

# List of resolved problems

## Resolved problems in R6301P02

None.

# Resolved problems in R6301P01

## 202212280349/202212021236

- Symptom: A VLAN interface fails to forward traffic at Layer 3 during an ISSU.
- Condition: This symptom occurs when an ISSU is performed.

# Resolved problems in R6301

## 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.

#### 201904020262

- Symptom: In an EVPN distributed relay environment, the interface where a single-armed AC is configured cannot forward packets.
- Condition: This symptom occurs if the IPP interface setting is cancelled and then restored for a tunnel interface .

#### 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.

#### 201903210720

- Symptom: In an EVPN distributed relay environment, the DR system sends out multiple copies of unknown unicast packets.
- Condition: This symptom might occur if the following operations have been performed:
  - a. Use a VXLAN tunnel as the IPL and reboot the DR system.
  - b. Receive unknown unicast packets from the remote AC.

#### 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.

#### 201903080004/201903070270

- Symptom: In an MPLS network, a P device drops packets continuously.
- Condition: This symptom might occur if the link between the P device and another P device or a PE device flaps for a long time more than once.

#### 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.

#### 201902140542

- Symptom: In an EVPN distributed relay environment, the IPL cannot work correctly.

- Condition: This symptom might occur if you configure VLAN-based VXLAN assignment and then configure EVPN distributed relay.

#### 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.

#### 201812110026

- Symptom: In an EVPN network, an access port sends packets with VLAN tags.
- Condition: This symptom might occur if two route reflectors are used and link switchover between them has occurred.

#### 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.



#### **201902010459**

- Symptom: CVE-2018-5407
- Condition: 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.

#### **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.

#### **201811230657**

- Symptom: CVE-2018-15473
- Condition: 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.

#### **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.

#### **201903280399**

- Symptom: When EVPN and DRNI are used together on the switch, frequent tunnel interface flapping might cause traffic interruption.
- Condition: This symptom might occur if frequent tunnel interface flapping occurs.

## **Resolved problems in F6207**

#### **201808290235**

- Symptom: Symmetric load sharing might not take effect.
- Condition: This symptom occurs if symmetric load sharing is configured on the device.

#### **201811010044**

- Symptom: The panel of the LSWM116Q interface module is displayed incorrectly on IMC.
- Condition: This symptom occurs if the LSWM116Q interface module is installed in subslot 4 of the device and managed by IMC.

#### **201811090022**

- Symptom: When an aggregation group has more than eight member ports, the excessive member ports do not have traffic.
- Condition: This symptom occurs if more than eight ports on a single device are added to an aggregation group and the corresponding aggregate interface receives unknown unicast traffic.

#### **201811130637**

- Symptom: When a specific port acts as the monitor port of Layer 2 remote port mirroring, no traffic is mirrored to the monitor port.
- Condition: This symptom occurs if the following conditions exist:
  - a. On an IRF fabric, Layer 2 remote port mirroring is configured.

- b. In the remote probe VLAN, the monitor port and the reflector port reside on different IRF member devices and have the same port number.

#### 201812050136

- Symptom: CVE-2018-15473
- Condition: 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.

#### 201812190652

- Symptom: A PBR policy fails to be applied because the ACL resources are insufficient.
- Condition: This symptom occurs if the following conditions exist:
  - a. The PBR policy is applied to interfaces belonging to different interface groups.
  - b. When you apply the PBR policy, the next hop of the PBR policy does not exist in the routing table.
  - c. The next hop of the PBR policy becomes reachable in the routing table.

#### 201812270200

- Symptom: A 40-GE interface is split into 10-GE breakout interfaces, and these 10-GE interfaces are configured as Layer 3 interfaces. Some breakout interfaces might be in an incorrect STP state and fail to learn ARP entries.
- Condition: This symptom occurs if the following operations are performed:
  - a. Split a 40-GE interface into 10-GE breakout interfaces.
  - b. Configure these 10-GE breakout interfaces as Layer 3 interfaces.

#### 201812290518

- Symptom: Layer 3 packets sent out of a specific interface are dropped.
- Condition: This symptom occurs if a specific interface forwards Layer 3 packets.

#### 201901110111

- Symptom: The CPU usage of the COPPD process becomes high.
- Condition: This symptom occurs if the following conditions exist:
  - a. Configure the RSVP protocol, and enable BFD for RSVP.
  - b. The device resides in the middle of the tunnel, and the downstream device is unreachable.

#### 201901110113

- Symptom: The Comsh task remains, and the CPU usage becomes high.
- Condition: This symptom occurs if the following operations are performed:
  - a. Log in to the device through Telnet.
  - b. Use the **lock-key** command to set the user line locking key.
  - c. Press this shortcut key to lock the remote connection.
  - d. Disconnect the remote connection when the remote connection is still locked.

#### 201901170294

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

# Resolved problems in F6206

## 201708310741

- Symptom: In a DRNI network, the keepalive link goes down.
- Condition: This symptom occurs if the device is configured with both DRNI and OpenFlow.

## 201712180820

- Symptom: In an EVPN DRNI network, the downlink interface receives redundant traffic.
- Condition: This symptom occurs if a DR interface on a DR device is shut down when the downlink host is silent.

## 201807120129

- Symptom: MPLS traffic cannot be forwarded.
- Condition: This symptom occurs if the following conditions exist in a CTOC network:
  - a. Primary and backup tunnels are configured.
  - b. The traffic is switched to the backup tunnel when a node fails.
  - c. The traffic is switched back to the primary tunnel when the link restores.

## 201807190749

- Symptom: CRC error packets appear when FC traffic is being forwarded.
- Condition: This symptom occurs if a 16G FC module is used to transmit the FC traffic.

## 201801190600

- Symptom: 10-GE interfaces on the LSWM124XG2Q and LSWM124XG2QFC interface modules do not come up.
- Condition: This symptom occurs if the HPE FlexFabric 5950 4-slot Switch has LSWM124XG2Q and LSWM124XG2QFC interface modules installed.

## 201806120020

- Symptom: The RSVP process exits exceptionally after certain operations.
- Condition: This symptom occurs if the public network tunnels are configured with TE FRR and IP address conflicts exist in a CTOC network.

## 201806120097

- Symptom: The device might reboot unexpectedly at a low probability.
- Condition: This symptom occurs if the HPE FlexFabric 5950 4-slot Switch uses an LSWM116Q interface module.

## 201805220109

- Symptom: When an IRF physical interface goes down, the other interfaces in the same group as the IRF physical interface flap.
- Condition: This symptom occurs if a 40-GE interface on an LSWM116Q interface module of the HPE FlexFabric 5950 4-slot Switch is used as an IRF physical interface.

## 201803190071

- Symptom: When ACLs are issued to multiple Layer 3 aggregate interfaces, the ACLs take effect on only one Layer 3 aggregate interface.
- Condition: This symptom occurs if ACLs are issued to multiple Layer 3 aggregate interfaces and rules are added to or deleted from these ACLs.

#### **201803170047**

- Symptom: Issued ACLs might not take effect.
- Condition: This symptom occurs if ACLs are repeatedly issued or repeatedly dynamically modified.

#### **201802050250**

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if the **shutdown** and **undo shutdown** commands are executed on the FC interface connecting to a server or storage device.

#### **201711290143**

- Symptom: A user cannot come online.
- Condition: This symptom occurs if the switch is configured to operate in FCF mode.

#### **201803290351**

- Symptom: PFC deadlock detection takes effect only on the first interface where it is configured, and does not take effect on the subsequent interfaces where it is configured.
- Condition: This symptom occurs if PFC deadlock detection is configured on two or more interfaces of the device.

#### **201711030407**

- Symptom: CVE-2017-1000253
- Condition: Local attackers may exploit this issue to gain root privileges.

#### **201712220137**

- Symptom: CVE-2017-3736
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

#### **201712190381**

- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.
- Symptom: CVE-2017-12192
- Condition: 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.
- Symptom: CVE-2017-15274
- Condition: An attacker can exploit this issue to cause a local denial-of-service condition.
- Symptom: CVE-2017-15299
- Condition: An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.

#### **201802060169**

- Symptom: CVE-2017-15896
- Condition: An attacker can exploit this issue to bypass TLS validate and encrypt, send application data to Node.js.
- Symptom: CVE-2017-3737
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.
- Symptom: CVE-2017-3738

- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

#### **201805250759**

- Symptom: CVE-2016-9586
- Condition: Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

#### **201710180649**

- Symptom: MACsec connections cannot be set up if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.
- Condition: This symptom might occur if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.

#### **201710240487**

- Symptom: EVPN traffic forwarding fails if the remote VTEP switches between tunnels.
- Condition: This symptom might occur if the remote VTEP switches between tunnels.

#### **201710270200**

- Symptom: An interface cannot forward traffic after its MACsec configuration is removed.
- Condition: This symptom might occur if MACsec configuration is removed from an interface.

#### **201706270683**

- Symptom: NetStream fails to collect traffic statistics on an interface when NetStream is disabled on other interfaces.
- Condition: This symptom occurs if NetStream is configured on multiple interfaces and then NetStream is disabled on one of these interfaces.

#### **201609230034**

- Symptom: BFD session flapping occurs when SSL VPN AC interfaces are shut down.
- Condition: This symptom might occur if SSL VPN AC interfaces are shut down.

#### **201708310704**

- Symptom: A 10-GE copper interface cannot come up.
- Condition: This symptom occurs if an external loopback test is performed on the 10-GE copper interface.

#### **201709260138**

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

#### **201711270371**

- Symptom: The management Ethernet interface might fail to be pinged.
- Condition: This symptom occurs if a master/subordinate switchover occurs to an IRF fabric.

## **Resolved problems in R6205P03**

#### **201709260138**

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

#### 201710180649

- Symptom: MACsec connections cannot be set up if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.
- Condition: This symptom might occur if a transceiver module or subcard is removed and re-installed when MACsec traffic exists.

#### 201710240487

- Symptom: EVPN traffic forwarding fails if the remote VTEP switches between tunnels.
- Condition: This symptom might occur if the remote VTEP switches between tunnels.

#### 201710270200

- Symptom: An interface cannot forward traffic after its MACsec configuration is removed.
- Condition: This symptom might occur if MACsec configuration is removed from an interface.

#### 201706270683

- Symptom: NetStream fails to collect traffic statistics on an interface when NetStream is disabled on other interfaces.
- Condition: This symptom occurs if NetStream is configured on multiple interfaces and then NetStream is disabled on one of these interfaces.

#### 201609230034

- Symptom: BFD session flapping occurs when SSL VPN AC interfaces are shut down.
- Condition: This symptom might occur if SSL VPN AC interfaces are shut down.

#### 201708310704

- Symptom: A 10-GE copper interface cannot come up.
- Condition: This symptom occurs if an external loopback test is performed on the 10-GE copper interface.

## Resolved problems in F6205P02

#### 201706050458

- Symptom: In an EVPN network, traffic is duplicated.
- Condition: This symptom occurs if the following conditions exist:
  - In an EVPN network, the outgoing interface of a VXLAN tunnel is a Layer 3 aggregate interface.
  - The **shutdown** or **undo shutdown** command is executed on an interface transmitting traffic.

#### 201706090010

- Symptom: Residual rawip sockets exist and occupy the memory.
- Condition: This symptom occurs if the switch performs NQA operations for a long time.

#### 201705250358

- Symptom: An FC aggregate interface cannot come up.
- Condition: This symptom occurs if the member ports of the FC aggregate interface are all on subordinate IRF member devices.

#### 201705060255

- Symptom: NetStream fails to collect traffic statistics on an interface.

- Condition: This symptom occurs if IPv6 NetStream filtering is enabled on the interface.

#### 201609060180

- Symptom: The following symptoms occur on an interface that hosts an AC:
  - If the priority trust mode is not set, the interface cannot perform EXP value mapping correctly for MPLS packets with an EXP value of 0, and the 802.1p priority of the packets is set to 0 after priority mapping.
  - If the priority trust mode is set to 802.1p or DSCP, the 802.1p priority of packets is set to 0 after priority mapping.
- Condition: This symptom might occur if the priority trust mode is not set or the **qos trust dot1p** or **qos trust dscp** command is executed on an interface that hosts an AC.

#### 201708250543

- Symptom: On a DR interface, traffic among different service instances associated with the same VSI cannot be forwarded.
- Condition: This symptom occurs if the DR interface is configured with ACs and the **shutdown** and **undo shutdown** commands are executed on the member ports of the DR interface.

#### 201708310748

- Symptom: NetStream fails to collect traffic statistics on an interface.
- Condition: This symptom occurs if IPv6 NetStream filtering is enabled on the interface.

#### 201709080177

- Symptom: A fiber management interface cannot come up.
- Condition: This symptom occurs if the transceiver module is removed from and then installed into a fiber management interface on a subordinate IRF member device.

#### 201708310760

- Symptom: MACsec cannot operate correctly on an MKA-enabled interface.
- Condition: This symptom occurs if the **speed** command is used to set the speed for an interface supporting MACsec.

## Resolved problems in F6205

#### 201705230173

- Symptom: On an EVPN network with distributed EVPN gateways, outgoing packets on an Ethernet service instance carry an 802.1Q VLAN tag unexpectedly.
- Condition: This symptom might occur if the device acts as an EVPN gateway to perform Layer 3 forwarding and the Ethernet service instance is configured to match frames that do not have an 802.1Q VLAN tag.

#### 201612050269

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7428

- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7431
- Condition: Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.

#### **201702220570**

- Symptom: CVE-2017-3730
- Condition: OpenSSL is prone to denial-of-service vulnerability. Attackers can exploit this issue to cause a denial-of-service condition.
- Symptom: CVE-2017-3731
- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to crash the application, resulting in denial-of-service condition.
- Symptom: CVE-2017-3732
- Condition: OpenSSL is prone to an information-disclosure vulnerability. An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

#### **201704280171**

- Symptom: CVE-2015-3405
- Condition: An attacker can exploit the ntp-keygen utility to spoof an NTP client or server.
- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.
- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

#### **201704280531**

- Symptom: CVE-2017-64558
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.
- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

## **Resolved problems in F6203**

#### **201704010616**

- Symptom: An IRF fabric splits when the IRF fabric has 8K VPLS PWs and the public network interface on the IRF fabric flaps.



- Condition: This symptom might occur if the IRF fabric has 8K VPLS PWs and the public network interface on the IRF fabric flaps.

#### **201703310499**

- Symptom: FNA is not available for GE interfaces on the FlexFabric 5950 48SFP28 8QSFP28 or FlexFabric 5950 4-slot switch.
- Condition: This symptom might occur if FNA is configured on GE interfaces of the FlexFabric 5950 48SFP28 8QSFP28 or FlexFabric 5950 4-slot switch.

#### **201704240426**

- Symptom: A memory exhaustion occurs on the switch when the switch is enabled with FNA and keeps generating notification messages for a long time.
- Condition: This symptom might occur if the switch is enabled with FNA and keeps generating notification messages for a long time.

#### **201703160569**

- Symptom: A 10-GE interface that is installed with a GE transceiver module and connected to another device cannot come up if the 10-GE interface is on one of the following hardware:
  - LSWM124XG2QL(JH180A) interface module.
  - FlexFabric 5950 32QSFP28 switch.
  - FlexFabric 5950 32QSFP28 TAA-compliant switch.
- Condition: This symptom might occur if the 10-GE interface is installed with a GE transceiver module and connected to another device and the 10-GE interface is on one of the following hardware:
  - LSWM124XG2QL(JH180A) interface module.
  - FlexFabric 5950 32QSFP28 switch.
  - FlexFabric 5950 32QSFP28 TAA-compliant switch.

#### **201704250571**

- Symptom: In an IRF fabric, forwarded Layer 2 packets arrive at the incoming interface of the packets again.
- Condition: This symptom occurs with a low probability if an interface in the IRF fabric is split into breakout interfaces and then the breakout interfaces are combined.

## **Resolved problems in F6202**

#### **201612050269**

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7428
- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers
- Symptom: CVE-2016-7431

- Condition: Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.

#### **201611030036**

- Symptom: Flow mirroring does not take effect.
- Condition: This symptom occurs if flow mirroring is configured in the outbound direction of a Layer 3 interface or Layer 3 aggregate interface.

## **Resolved problems in R6125**

#### **201610100291**

- Symptom: On a VXLAN or EVPN network, unknown unicast, broadcast, or multicast packets are duplicated or lost after they are forwarded.
- Condition: This symptom occurs if the Ethernet service instance of a VSI is created on a cross-chassis Layer 2 aggregate interface, of which member ports are on different IRF member devices.

#### **201612270330**

- Symptom: The system prompts that the memory is insufficient when the BGP neighborhood information is displayed.
- Condition: This symptom occurs if SNMP is used to read BGP information multiple times and causes memory leak.

#### **201610240176**

- Symptom: Inter-data center Layer 2 forwarding fails in an EVPN-DCI network.
- Condition: This symptom might occur if Layer 2 traffic is forwarded between two data centers of an EVPN-DCI network.

#### **201609060256**

- Symptom: Frequent LDP protocol flapping causes hardware nexthop entry leakage and forwarding failure.
- Condition: This symptom might occur if the LDP protocol flaps frequently.

#### **201610140317**

- Symptom: CVE-2016-6304
- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to cause a denial-of-service condition.
- Symptom: CVE-2016-6306
- Condition: OpenSSL is prone to a local denial-of-service vulnerability. A local attacker can exploit this issue to cause a denial-of-service condition.

#### **201611070341**

- Symptom: CVE-2016-8858
- Condition: A remote user can send specially crafted data during the key exchange process to trigger a flaw in `kex_input_kexinit()` and consume excessive memory on the target system. This can be exploited to consume up to 384 MB per connection.

#### **201611080162**

- Symptom: CVE-2016-5195

- Condition: An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

#### **201609140425**

- Symptom: After L2VPN is disabled, the EVPN-enabled device cannot forward traffic correctly because some EVPN ARP entries are not deleted.
- Condition: This symptom might occur if L2VPN is disabled on the EVPN-enabled device.

## **Resolved problems in R6123**

#### **201609180002**

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2106
- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.0.2h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.
- Symptom: CVE-2016-2108
- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).
- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
- Symptom: CVE-2016-2176
- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service.

#### **201607290021**

- Symptom: CVE-2016-2177
- Condition: Fixed vulnerability in s3\_srvr.c, ssl\_sess.c, and t1\_lib.c functions in OpenSSL through 1.0.2h that allows remote attackers to cause a denial of service (integer overflow and application crash), or possibly have an unspecified other impact by leveraging unexpected malloc behavior.

#### **201606240193**

- Symptom: CVE-2016-4953

- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.
- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.
- Symptom: CVE-2016-4956
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

#### **201609010406**

- Symptom: CVE-2009-3238
- Condition: The get\_random\_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms

#### **201603310333**

- Symptom: The port mirroring configuration fails to be issued.
- Condition: This symptom occurs if an aggregate interface is configured as the monitor port of a mirroring group.

#### **201604080607**

- Symptom: VXLAN traffic cannot be forwarded when the switch acts as a VXLAN IP gateway and has sFlow configured.
- Condition: This symptom occurs if sFlow is enabled on the physical interface corresponding to the VXLAN tunnel.

#### **201604140250**

- Symptom: In a VXLAN network, the routing protocols flap.
- Condition: This symptom occurs if the following conditions exist:
  - The switch acts as a VXLAN IP gateway.
  - A large number of VXLAN tunnels are created on the switch.
  - The switch is sending and receiving a large number of ARP packets.

#### **201604200574**

- Symptom: OSPF neighborhood flaps.
- Condition: This symptom occurs if an IRF splits.

#### **201512230507**

- Symptom: The configuration might fail to be saved.
- Condition: This symptom might occur if you save the configuration.

## **Resolved problems in R6106P01**

None.

# Resolved problems in R6106

## 201604060275

- Symptom: The PBR configuration on a VSI interface does not take effect.
- Condition: This symptom occurs if PBR is configured on a VSI interface of a VXLAN IP gateway.

## 201604010510

- Symptom: The DHCP snooping entries are not complete.
- Condition: This symptom occurs if both DHCP relay agent and DHCP snooping are configured on the switch in a Layer 3 network.

## 201604050208

- Symptom: The sub-VLANs of a super VLAN do not send IGMP/MLD queries.
- Condition: This symptom occurs if a super VLAN is configured and IGMP/MLD is configured on the VLAN interface of the super VLAN.

## 201603310127

- Symptom: Unknown unicast traffic and broadcast traffic are dropped in the outbound direction of an interface.
- Condition: This symptom occurs if the interface is configured as an IRF physical interface and then configured as a common interface.

# Resolved problems in R6105

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](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:  
[www.hpe.com/support/hpesc](http://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 FlexFabric 5950 Command References-Release 620x
- HPE FlexFabric 5950 Configuration Guides-Release 620x
- HPE FlexFabric 5950 Switch Series Installation Guide
- HPE X711 Frt(prt)-Bck(pwr) HV2 Fan Tray (JH388A) & HPE X712 Bck(pwr)-Frt(prt) HV2 Fan Tray (JH389A) User Guide
- HPE A58x0AF 650W AC (JC680A) & 650W DC (JC681A) Power Supplies User Guide
- HPE 5930-4Slot Fan Trays (JH185A & JH186A) User Guide
- HPE LSWM18CQ Interface Module (JH406A) User Guide
- HPE LSWM116Q Interface Module (JH405A) User Guide
- HPE LSWM124TG2H Interface Module (JH450A) User Guide
- HPE LSWM18QC Interface Module (JH183A) User Guide
- HPE LSWM124XG2Q & LSWM124XG2QL Interface Modules User Guide
- HPE LSWM124XGT2Q Interface Module (JH182A) User Guide
- HPE LSWM124XG2QFC Interface Module (JH184A) User Guide

## 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](mailto: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 Feature list

## Hardware features

**Table 5 5950 series hardware features**

Item	HPE FlexFabric 5950 32QSFP28 Switch JH321A  HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
Dimensions (H x W x D)	43.6 x 440 x 540 mm (1.72 x 17.32 x 21.26 in)	43.6x440x460 (1.72 x 17.32 x 18.11 in)	88.1x440x660 (1.72 x 17.32 x 25.98 in)
Weight	≤ 15.0 kg (33.07 lb)	≤ 15kg (33.07 lb)	≤ 18kg (39.68 lb)
Console ports	1		
Mini USB(Console)	1		
Management Ethernet ports	<ul style="list-style-type: none"> <li>10M/100M/1000M Base-T copper port: 1</li> <li>SFP port: 1</li> </ul>		
USB ports	1		
SFP ports	N/A	2	2
SFP+ ports	2	N/A	N/A
SFP28 ports	N/A	48	N/A
QSFP28 ports	32	8	N/A
Expansion cards	N/A	N/A	LSWM18CQ LSWM116Q LSWM124TG2H LSWM124XGT2Q LSWM124XG2QFC LSWM18QC LSWM124XG2Q LSWM124XG2QL LSWM18CQMSEC
Fan tray slots	6	5	2
Fan trays	HPE X712 Bck(pwr)-Frt(prt) HV2 Fan Tray (JH389A) HPE X711 Frt(prt)-Bck(pwr) HV2 Fan Tray (JH388A)	HPE X712 Bck(pwr)-Frt(prt) HV2 Fan Tray (JH389A) HPE X711 Frt(prt)-Bck(pwr) HV2 Fan Tray (JH388A)	HPE 5930 4-slot B(pwr) F(prt) Fan Tray(JH185A) HPE 5930 4-slot F(prt) B(pwr) Fan Tray(JH186A)
Power module slots	2	2	4
Power modules	A58x0AF 650W AC Power Supply (JC680A) A58x0AF 650W DC Power Supply (JC681A)		

Item	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
AC-input voltage	Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz		
DC-input voltage	Rated voltage: –48 VDC to –60 VDC Max voltage: –40 VDC to –72 VDC		
Minimum power consumption	Single-AC: 280W Dual-AC: 286W Single-DC: 270W Dual-DC: 275W	Single-AC: 188W Dual-AC: 200W Single-DC: 180W Dual-DC: 195W	Dual-AC: 180W Triple AC: 197W Quadruple AC: 213W Dual-DC: 187W Triple DC: 202W Quadruple DC: 213W
Maximum power consumption	Single-AC: 586W Dual-AC: 590W Single-DC: 582W Dual-DC: 572W	Single-AC: 405W Dual-AC: 413W Single-DC: 400W Dual-DC: 408W	Dual-AC: 612W Triple AC: 618W Quadruple AC: 635W Dual-DC: 610W Triple DC: 612W Quadruple DC: 613W
Chassis leakage current compliance	<ul style="list-style-type: none"> <li>• UL60950-1</li> <li>• EN60950-1</li> <li>• IEC60950-1</li> <li>• GB4943</li> </ul>		
Melting current of power supply fuse	<ul style="list-style-type: none"> <li>• 650W AC power supply: 10 A @ 250 VAC</li> <li>• 650W DC power supply: 30 A @ 250 VDC</li> </ul>		
Operating temperature	0°C to 45°C (32°F to 113°F)		
Operating humidity	10% to 90%, noncondensing		
Fire resistance compliance	<ul style="list-style-type: none"> <li>• UL60950-1</li> <li>• EN60950-1</li> <li>• IEC60950-1</li> <li>• GB4943</li> </ul>		



# Software features

**Table 6 Software features of the MSR 20/MSR 30/MSR 50 series**

Feature	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
Full duplex Wire speed L2 switching capacity	6400Gbps	4000Gbps	6400Gbps
Whole system Wire speed L2 switching Packet forwarding rate	3169.6Mpps	3169.6Mpps	3169.6Mpps
Forwarding mode	Store-forward and cut-through		
Link aggregation	<ul style="list-style-type: none"> <li>• Aggregation of 10-GE ports</li> <li>• Aggregation of 25-GE ports</li> <li>• Aggregation of 40-GE ports</li> <li>• Aggregation of 100-GE ports</li> <li>• Static link aggregation</li> <li>• Dynamic link aggregation</li> <li>• When stacked, supports up to 256 aggregation groups, each supporting up to 32 ports</li> </ul>		
Flow control	IEEE 802.3x flow control and back pressure		
Jumbo Frame	Supports maximum frame size of 9416		
MAC address table	<ul style="list-style-type: none"> <li>• 136K MAC addresses</li> <li>• 8K static MAC addresses</li> <li>• Blackhole MAC addresses</li> <li>• MAC address learning limit on a port</li> </ul>		
VLAN	<ul style="list-style-type: none"> <li>• Port-based VLANs (4094 VLANs)</li> </ul>		
QinQ	<ul style="list-style-type: none"> <li>• Supported</li> </ul>		
VLAN Mapping	<ul style="list-style-type: none"> <li>• 1;1 VLAN Mapping</li> <li>• 1:2 VLAN Mapping</li> <li>• 2:2 VLAN Mapping</li> </ul>		
ARP	<ul style="list-style-type: none"> <li>• 136K entries</li> <li>• 1K static entries</li> <li>• Gratuitous ARP</li> <li>• Standard proxy ARP and local proxy ARP</li> <li>• ARP source suppression</li> <li>• ARP black hole</li> <li>• ARP detection (based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings)</li> </ul>		
ND	<ul style="list-style-type: none"> <li>• 68K entries</li> <li>• 1K static entries</li> </ul>		
VLAN virtual interface	2K		

Feature	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
DHCP	<ul style="list-style-type: none"> <li>DHCP client</li> <li>DHCP snooping</li> <li>DHCP relay agent</li> <li>DHCP server</li> <li>DHCPv6 server</li> </ul>		
UDP helper	<ul style="list-style-type: none"> <li>Supported</li> </ul>		
DNS	<ul style="list-style-type: none"> <li>Dynamic domain name resolution</li> <li>Dynamic domain name resolution client</li> <li>IPv4/IPv6 addresses</li> </ul>		
IPv4 routing	<ul style="list-style-type: none"> <li>4K static routes</li> <li>RIP(Routing Information Protocol) v1/v2; up to 4K IPv4 routes</li> <li>OSPF (Open Shortest Path First) v1/v2; up to 128K IPv4 routes</li> <li>IS-IS(Intermediate System to Intermediate system); up to 128K IPv4 routes</li> <li>BGP (Border Gateway Protocol); up to 128K IPv4 routes</li> <li>Configurable maximum number of equal-cost routes; up to 2K equal-cost routes</li> <li>Routing policy</li> <li>VRRP</li> <li>PBR</li> </ul>		
IPv6 routing	<ul style="list-style-type: none"> <li>2K static routes</li> <li>RIPng: Supports up to 2K IPv6 routes</li> <li>OSPF v3: Supports up to 84K IPv6 routes</li> <li>IPv6 IS-IS: Supports up to 84K IPv6 routes</li> <li>BGP4+: Supports up to 84K IPv6 routes</li> <li>Up to 2K ECMP routes; each ECMP route supports up to 128 next hops</li> <li>Routing policy</li> <li>VRRP</li> <li>PBR</li> </ul>		
Multicast	<ul style="list-style-type: none"> <li>IGMP snooping</li> <li>MLD snooping</li> <li>IPv4 and IPv6 multicast VLAN</li> <li>IPv4 and IPv6 PIM snooping</li> <li>IGMP and MLD</li> <li>PIM and IPv6 PIM</li> <li>MSDP</li> <li>Multicast VPN</li> </ul>		

Feature	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
MPLS	<ul style="list-style-type: none"> <li>• Static LSP</li> <li>• LDP</li> <li>• MPLS TE</li> <li>• Static CRLSP</li> <li>• RSVP</li> <li>• Tunnel policy</li> <li>• MPLS OAM</li> <li>• MPLS L3VPN</li> <li>• MCE</li> </ul>		
BFD	<ul style="list-style-type: none"> <li>• RIP/RIPng</li> <li>• OSPF/OSPFv3</li> <li>• IS-IS/IPv6 IS-IS</li> <li>• BGP/BGP4+</li> <li>• Static route/IPv6 static route</li> </ul>		
Tunnel	<ul style="list-style-type: none"> <li>• IPv4 over IPv4 tunnel</li> <li>• IPv4 over IPv6 tunnel</li> <li>• IPv6 over IPv4 manual tunnel</li> <li>• IPv6 over IPv4 6to4 tunnel</li> <li>• IPv6 over IPv4 ISATAP tunnel</li> <li>• IPv6 over IPv6 tunnel</li> <li>• GRE tunnel</li> </ul>		
MSTP	<ul style="list-style-type: none"> <li>• STP/RSTP/MSTP protocol</li> <li>• STP Root Guard</li> <li>• BPDU Guard</li> </ul>		
QoS/ACL	<ul style="list-style-type: none"> <li>• Restriction of the rates at which a port sends and receives packets, with a granularity of 8 kbps.</li> <li>• Packet redirect</li> <li>• Committed access rate (CAR), with a granularity of traffic limit 8 kbps.</li> <li>• Eight output queues for each port</li> <li>• Flexible queue scheduling algorithms based on port and queue, including strict priority (SP), Weighted Deficit Round Robin (WDRR), Weighted Fair Queuing (WFQ), SP + WDRR, and SP + WFQ.</li> <li>• Remarking of 802.1p and DSCP priorities</li> <li>• Packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN.</li> <li>• Time range</li> <li>• Weighted Random Early Detection (WRED)</li> <li>• Queue shaping</li> <li>• User profile</li> <li>• COPP</li> <li>• Explicit Congestion Notification (ECN)</li> </ul>		

Feature	HPE FlexFabric 5950 32QSFP28 Switch JH321A HPE FlexFabric 5950 32QSFP28 TAA-compliant Switch JH322A	HPE FlexFabric 5950 48SFP28 8QSFP28 Switch JH402A	HPE FlexFabric 5950 4-slot Switch JH404A
Mirroring	<ul style="list-style-type: none"> <li>Flow mirroring</li> <li>Port mirroring</li> <li>Multiple mirror observing port</li> </ul>		
Remote mirroring	<ul style="list-style-type: none"> <li>Port remote mirroring (RSPAN)</li> </ul>		
Security	<ul style="list-style-type: none"> <li>Hierarchical management and password protection of users</li> <li>AAA authentication</li> <li>RADIUS</li> <li>HWTACACS</li> <li>SSH 2.0</li> <li>PKI</li> <li>SSL</li> <li>HTTPs</li> <li>Attack detection and prevention</li> <li>IP Source Guard</li> <li>uRPF</li> <li>Keychain</li> </ul>		
Traffic Management	<ul style="list-style-type: none"> <li>sFlow</li> <li>Netstream(HPE FlexFabric 5950 48SFP28 8QSFP28 Switch and HPE FlexFabric 5950 4-slot Switch)</li> </ul>		
Loading and upgrading	<ul style="list-style-type: none"> <li>Loading and upgrading through XModem protocol</li> <li>Loading and upgrading through FTP</li> <li>Loading and upgrading through the trivial file transfer protocol (TFTP)</li> </ul>		
Management	<ul style="list-style-type: none"> <li>Configuration at the command line interface</li> <li>Remote configuration through Telnet</li> <li>Configuration through Console port</li> <li>Simple network management protocol (SNMP)</li> <li>System log</li> <li>Hierarchical alarms</li> <li>NTP</li> <li>Power supply alarm function</li> <li>Fan and temperature alarms</li> </ul>		
Maintenance	<ul style="list-style-type: none"> <li>Debugging information output</li> <li>Ping and Tracert</li> <li>Remote maintenance through Telnet</li> <li>DLDP</li> <li>File download and upload through USB port</li> </ul>		

# Appendix B Upgrading software

The following information describes how to upgrade 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."

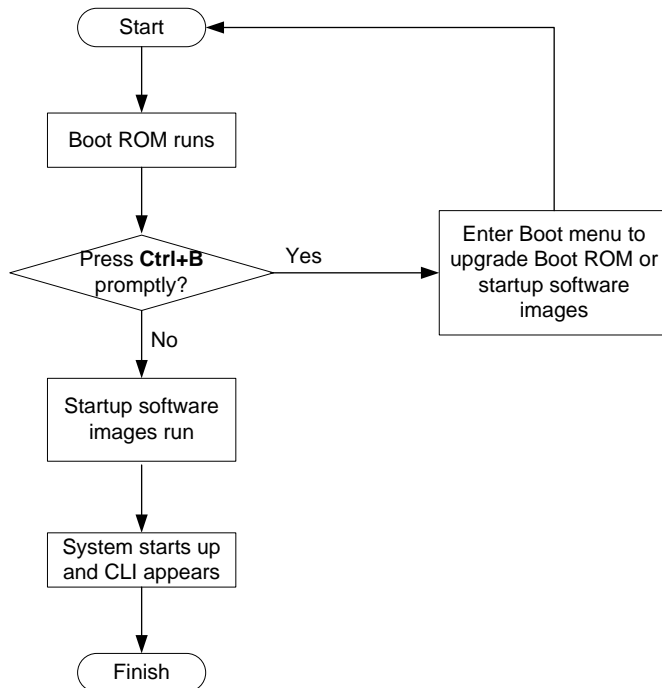
These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images in the file and sets them as startup software images. Typically, the Boot ROM and software images for this switch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

In addition to these images, HP 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	<ul style="list-style-type: none"> <li>You must reboot the switch to complete the upgrade.</li> <li>This method can interrupt ongoing network services.</li> </ul>
	Patch packages	<p>The upgrade does not interrupt ongoing services.</p> <p>Make sure the patch packages match the current software images. A patch package can fix bugs only for its matching software image version.</p>
Upgrading from the Boot menu	<ul style="list-style-type: none"> <li>Boot ROM image</li> <li>Software images</li> </ul>	<p>Use this method when the switch cannot correctly start up.</p> <p><b>⚠ CAUTION:</b></p> <p>Upgrading an IRF fabric from the CLI rather than the Boot menu.</p> <p>The Boot menu approach requires that you upgrade the member switches one by one and has larger impact on services than the CLI approach.</p>

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, 5950-cmw710-boot-r6105.bin and 5950-cmw710-system-r6105.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** command deletes a file permanently and the action cannot be undone.
- The **delete file** 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** 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.
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> system-view
[Sysname] ftp server enable

[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 5950 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 the file flash:/newest.ipe on slot 1....Done..
```

```
Images in IPE:
```

```
boot.bin
```

```
system.bin
```

```
Decompressing file boot.bin to flash:/boot.bin.....Done.
```

```
Decompressing file system.bin to
flash:/system.bin.....Done.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software images for
all slots.
Do you want to delete flash:/newest.ipe now? [Y/N]:n
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1...Done.
The images that have passed all examinations will be used as the backup 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 the file flash:/newest.ipe on slot 2....Done..
Images in IPE:
    boot.bin
    system.bin
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to
flash:/system.bin.....Done.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software images for
all slots.
Do you want to delete flash:/newest.ipe now? [Y/N]:n
Verifying the file flash:/boot.bin on slot 2...Done.
Verifying the file flash:/system.bin on slot 2...Done.
The images that have passed all examinations will be used as the backup 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 HP FlexFabric 5950 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 HP FF 5950-32QSFP28 Switch), and you can see the following information:

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

*****
*                                                                 *
*          HPE FF 5950 32QSFP28 Switch BOOTROM, Version 106      *
*                                                                 *
*****

Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP

Creation Date       : Apr  7 2016
CPU Type           : P2020
CPU L1 Cache       : 32KB
CPU Clock Speed    : 1200MHz
Memory Type        : DDR3 SDRAM
Memory Size        : 4096MB
Memory Speed       : 800MHz
Flash Size         : 1024MB
CPLD Version       : 1.0
PCB Version        : Ver.B
Mac Address        : 6000D246D4F8
```

Press Ctrl+B to access EXTENDED BOOT MENU...0

Press one of the shortcut key combinations at prompt.

**Table 7 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.

Shortcut keys	Prompt message	Function	Remarks
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 101
*
*****
```

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 8 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 <a href="#">Using XMODEM to upgrade Boot ROM through the console port</a> .
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 <a href="#">Using XMODEM to upgrade Boot ROM through the console port</a> .
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 <a href="#">Using XMODEM to upgrade Boot ROM through the console port</a> .

Option	Task
	<a href="#">console port</a> .
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see <a href="#">Accessing the extended Boot menu</a> .
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press <b>Ctrl + U</b> to access the BASIC ASSISTANT menu (see <a href="#">Table 9</a> ).

**Table 9 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 10](#)). For more information about password recovery capability, see *HP FlexFabric 5950 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+R: Download image to SDRAM and run

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



**Table 10 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	<ul style="list-style-type: none"> <li>Specify the main and backup software image file for the next startup.</li> <li>Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.</li> </ul>
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	<p>Delete the current next-startup configuration files and restore the factory-default configuration.</p> <p>This option is available only if password recovery capability is disabled.</p>
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	<p>Start the switch without loading any configuration file.</p> <p>This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option.</p> <p>This option is available only if password recovery capability is enabled.</p>
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	<p>Skip the authentication for console login.</p> <p>This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option.</p> <p>This option is available only if password recovery capability is enabled.</p>
Ctrl+R: Download image to SDRAM and run	<p>Download a system software image and start the switch with the image.</p> <p>This option is available only if password recovery capability is enabled.</p>
Ctrl+Z: Access EXTENDED ASSISTANT MENU	<p>Access the EXTENDED ASSISTANT MENU.</p> <p>For options in the menu, see <a href="#">Table 11</a>.</p>

**Table 11 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

- Enter **1** in the Boot menu to access the file transfer protocol submenu.
  - Set TFTP protocol parameters
  - Set FTP protocol parameters
  - 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 12 TFTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.ipe</b> ).
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+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 13 FTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.ipe</b> ).
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+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.

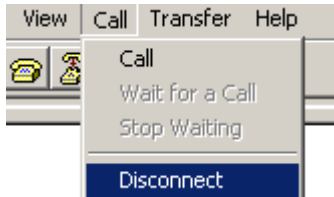
Download baudrate is 115200 bps

Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

Press enter key when ready

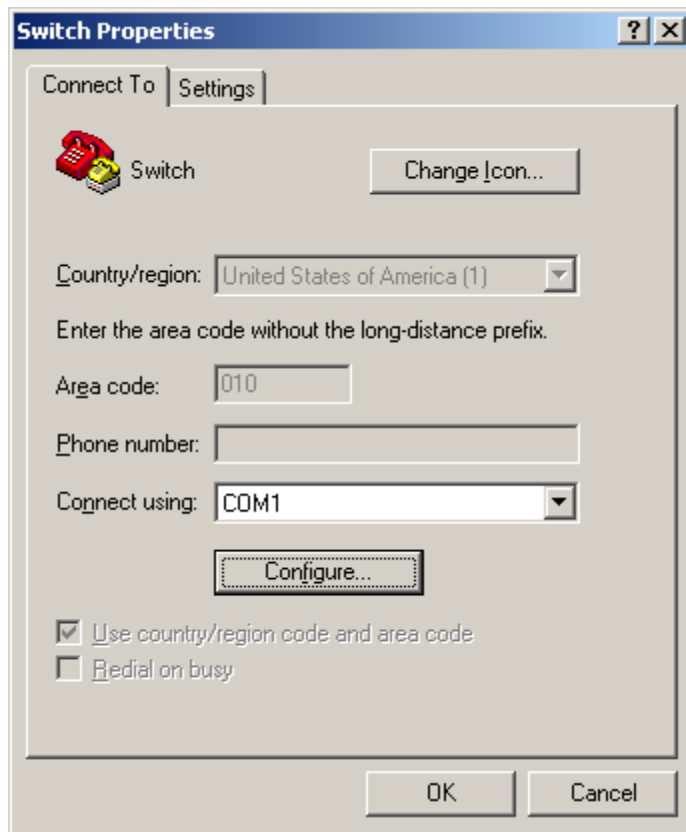
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
5. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

**Figure 2 Disconnecting the terminal from the switch**



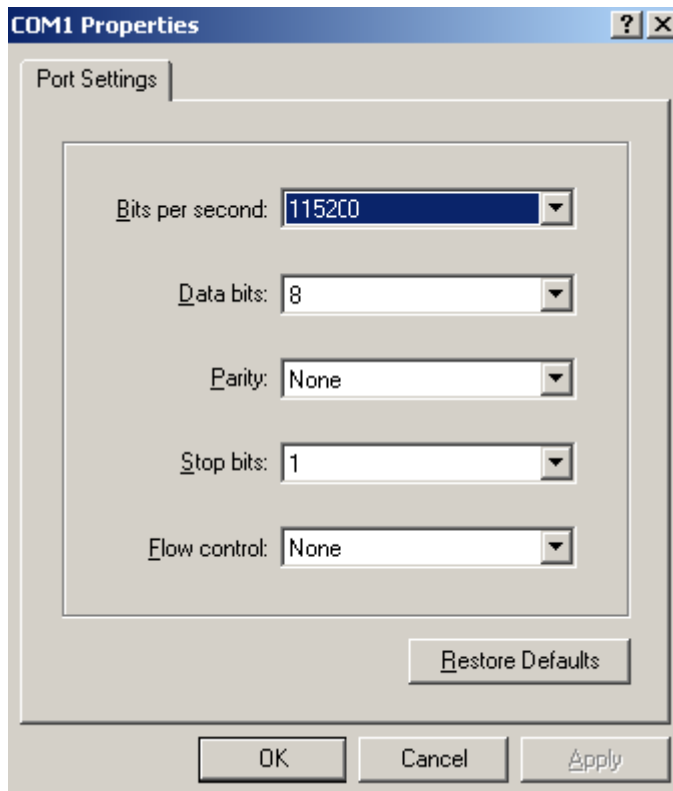
6. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

**Figure 3 Properties dialog box**



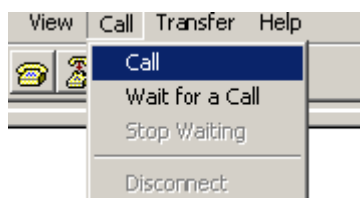
7. Select **115200** from the **Bits per second** list and click **OK**.

**Figure 4 Modifying the baud rate**



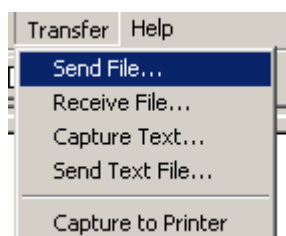
8. Select **Call > Call** to reestablish the connection.

**Figure 5 Reestablishing the connection**



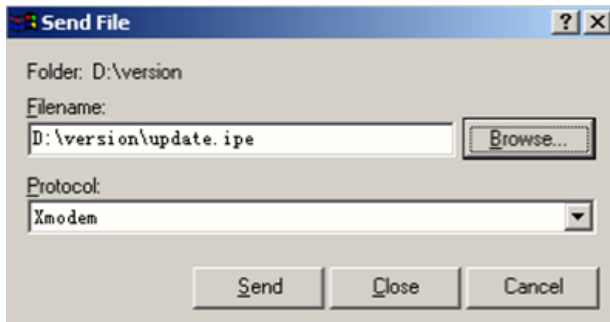
9. Press **Enter**. The following prompt appears:  
Are you sure to download file to flash? Yes or No (Y/N):Y
10. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)  
Now please start transfer file with XMODEM protocol  
If you want to exit, Press <Ctrl+X>  
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
11. Select **Transfer > Send File** in the HyperTerminal window.

**Figure 6 Transfer menu**



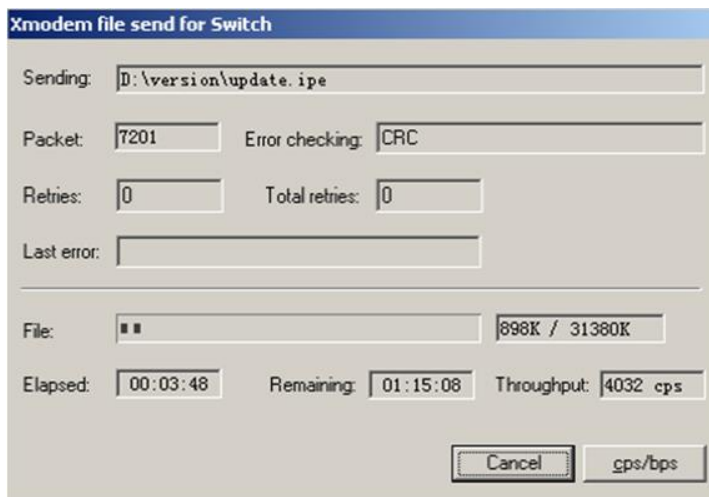
12. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

**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+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 14 TFTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.btm</b> ).
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.

**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 15 FTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.btm</b> ).
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.

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.

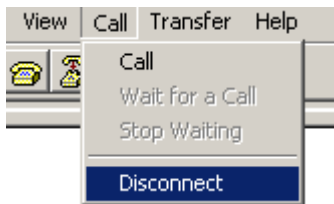
Download baudrate is 115200 bps

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.

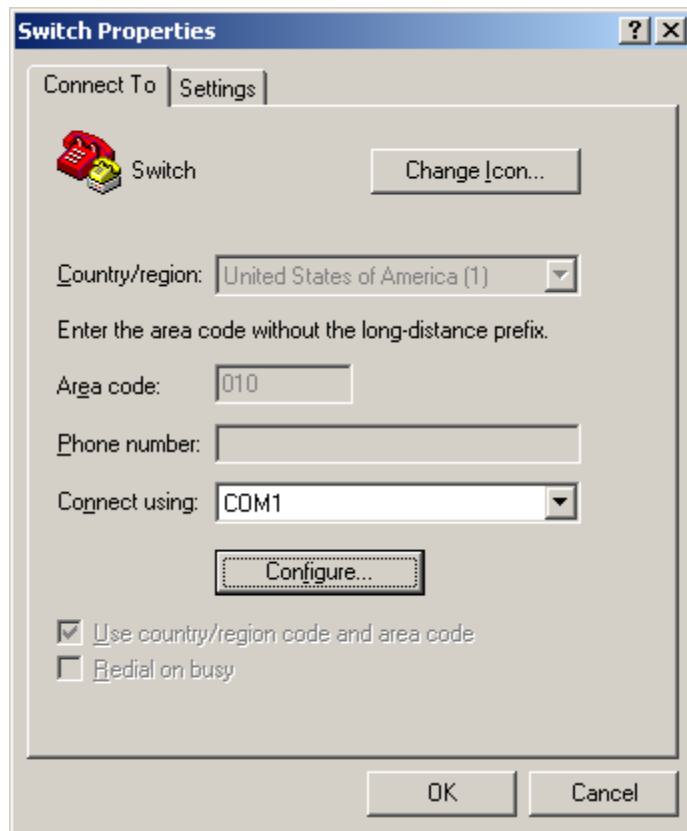
6. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

**Figure 9 Disconnecting the terminal from the switch**



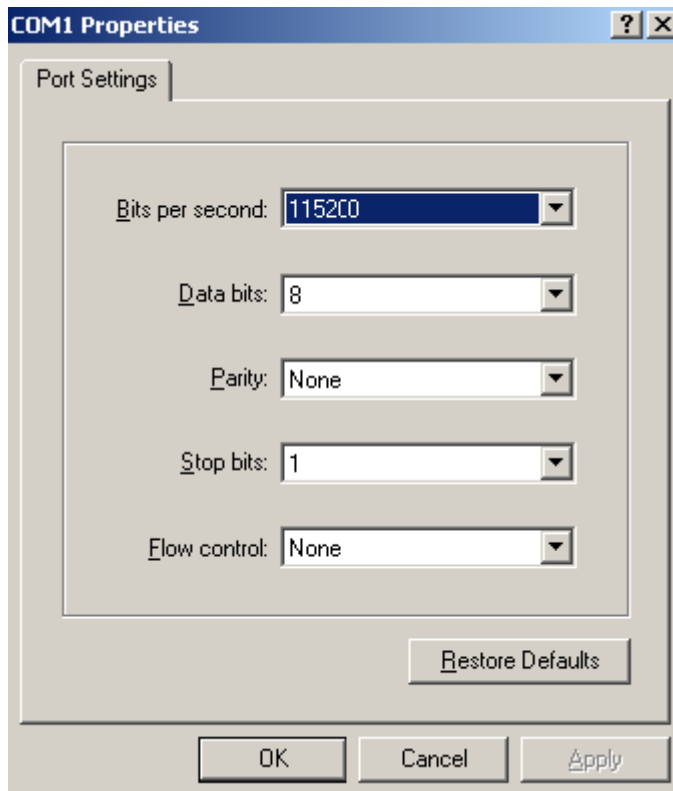
7. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

**Figure 10 Properties dialog box**



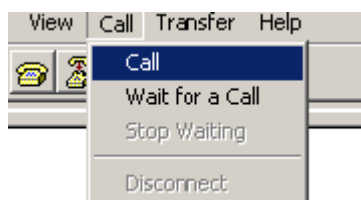
8. Select **115200** from the **Bits per second** list and click **OK**.

**Figure 11 Modifying the baud rate**



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

**Figure 12 Reestablishing the connection**

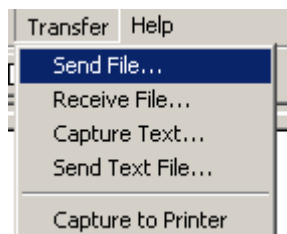


10. Press **Enter** to start downloading the file.

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

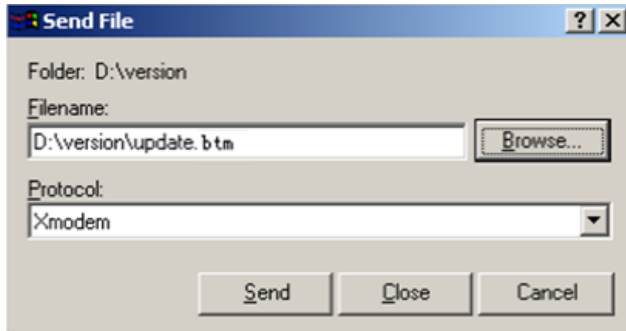
11. Select **Transfer > Send File** in the HyperTerminal window.

**Figure 13 Transfer menu**



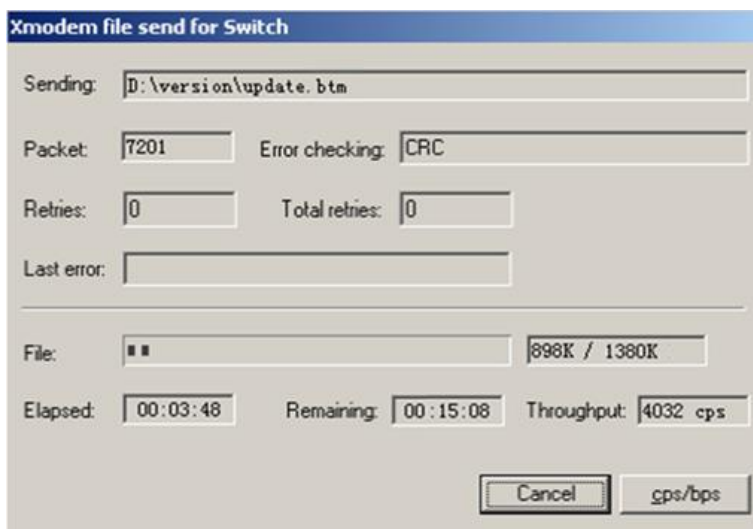
12. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

**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+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+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 5950-CMW710-R6301P02 Release Notes

## Software Feature Changes

The information in this document is subject to change without notice.  
© Copyright 2023 Hewlett Packard Enterprise Development LP

# Contents

About software feature changes .....	1
Release 6301P02.....	2
Release 6301P01.....	3
Release 6301 .....	4
New features: Fundamentals features .....	6
New features: Virtual technologies features .....	7
New features: Layer 2—LAN switching features.....	7
New features: Layer 3—IP services features .....	9
New features: Layer 3—IP routing features.....	13
New features: IP multicast features .....	18
New features: MPLS features .....	20
New features: ACL and QoS features .....	21
New features: Security features.....	23
New features: High availability features.....	28
New features: Network management and monitoring features.....	29
New features: FC and FCoE features .....	31
New features: OpenFlow features .....	31
New features: VXLAN features.....	32
New features: EVPN features .....	32
Modified feature: ISSU by using issu commands.....	33
Feature change description .....	33
Command changes .....	34
Modified command: display version comp-matrix.....	34
Modified command: issu load.....	34
Modified command: issu one-step.....	35
Modified feature: Automatic configuration .....	35
Feature change description .....	35
Command changes .....	35
Modified feature: Setting the timestamp format for logs sent to log hosts....	36
Feature change description .....	36
Command changes .....	36
Modified command: info-center timestamp loghost .....	36

<b>Modified feature: Configuring an interface event for a CLI-defined EAA monitor policy .....</b>	<b>36</b>
Feature change description .....	36
Command changes .....	36
Modified command: event-interface .....	36
<b>Modified feature: Configuring an EAA monitor policy by using Tcl .....</b>	<b>37</b>
Feature change description .....	37
Command changes .....	37
<b>Modified feature: Displaying the operating status and information of an interface .....</b>	<b>37</b>
Feature change description .....	37
Command changes .....	37
Modified command: display interface .....	37
<b>Modified feature: Displaying PFC information of all interfaces .....</b>	<b>38</b>
Feature change description .....	38
Command changes .....	38
Modified command: display priority-flow-control interface .....	38
<b>Modified feature: Link state change suppression on an interface .....</b>	<b>39</b>
Feature change description .....	39
Command changes .....	39
Modified command: link-delay .....	39
<b>Modified feature: MAC-to-VLAN entries .....</b>	<b>40</b>
Feature change description .....	40
Command changes .....	40
Modified command: mac-vlan mac-address .....	40
Modified command: display mac-vlan .....	40
<b>Modified feature: Collision handling process of LACP MAD and BFD MAD ..</b>	<b>41</b>
Feature change description .....	41
Command changes .....	41
<b>Modified feature: Collision handling process of ND MAD .....</b>	<b>42</b>
Feature change description .....	42
Command changes .....	42
<b>Modified feature: Displaying global link aggregation load sharing modes ....</b>	<b>42</b>
Feature change description .....	42
Command changes .....	42
Modified command: display link-aggregation load-sharing mode .....	42
<b>Modified feature: Configuring a link aggregation load sharing hash seed ....</b>	<b>43</b>
Feature change description .....	43
Command changes .....	43
Modified command: link-aggregation global load-sharing seed .....	43
<b>Modified feature: Displaying detailed information about the IPP and DR interfaces of DRNI .....</b>	<b>44</b>
Feature change description .....	44
Command changes .....	44
Modified command: display drni verbose .....	44
<b>Modified feature: Configuring the advertisable TLVs for LLDP .....</b>	<b>45</b>
Feature change description .....	45
Command changes .....	46

Modified command: lldp tlv-enable .....	46
<b>Modified feature: Setting the aging timer for dynamic ARP entries .....</b>	<b>51</b>
Feature change description .....	51
Command changes .....	51
Modified command: arp timer aging .....	51
<b>Modified feature: ARP snooping .....</b>	<b>52</b>
Feature change description .....	52
Command changes .....	52
Modified command: arp snooping enable .....	52
Modified command: display arp snooping .....	52
Modified command: reset arp snooping .....	53
<b>Modified feature: Specifying DHCP servers for a DHCP relay address pool .....</b>	<b>53</b>
Feature change description .....	53
Command changes .....	53
Modified command: remote-server .....	53
<b>Modified feature: Displaying DHCP snooping and DHCPv6 snooping trusted ports .....</b>	<b>54</b>
Feature change description .....	54
Command changes .....	54
Modified command: display dhcp snooping trust .....	54
Modified command: display ipv6 dhcp snooping trust .....	55
<b>Modified feature: Displaying DHCP address pool information .....</b>	<b>57</b>
Feature change description .....	57
Command changes .....	57
Modified command: display dhcp server pool .....	57
<b>Modified feature: Displaying DHCPv6 address pool information .....</b>	<b>59</b>
Feature change description .....	59
Command changes .....	59
Modified command: display ipv6 dhcp pool .....	59
<b>Modified feature: Enabling recording DHCPv6 snooping address entries in VLAN view .....</b>	<b>61</b>
Feature change description .....	61
Command changes .....	62
Modified command: ipv6 dhcp snooping binding record .....	62
<b>Modified feature: Setting the aging timer for ND entries in stale state .....</b>	<b>62</b>
Feature change description .....	62
Command changes .....	62
<b>Modified feature: Displaying member interfaces shut down by Monitor Link .....</b>	<b>62</b>
Feature change description .....	62
Command changes .....	63
Modified command: display monitor-link group .....	63
<b>Modified feature: Displaying DLDP configuration .....</b>	<b>63</b>
Feature change description .....	63
Command changes .....	63
Modified command: display dldp .....	63
<b>Modified feature: Configuring routing policy-based recursive lookup .....</b>	<b>64</b>
Feature change description .....	64
Command changes .....	64
Modified command: protocol nexthop recursive-lookup .....	64

Modified feature: Associating Track with the output interface for a static route .....	65
Feature change description .....	65
Command changes .....	65
Modified command: ip route-static .....	65
Modified feature: Configuring OSPF area authentication .....	66
Feature change description .....	66
Command changes .....	66
Modified command: authentication-mode .....	66
Modified feature: Configuring OSPF interface authentication .....	67
Feature change description .....	67
Command changes .....	67
Modified command: ospf authentication-mode .....	67
Modified feature: Configuring a virtual link .....	68
Feature change description .....	68
Command changes .....	68
Modified command: vlink-peer .....	68
Modified feature: Setting the number of OSPF logs .....	68
Feature change description .....	68
Command changes .....	69
Modified command: event-log .....	69
Modified feature: Displaying IS-IS LSP log information .....	69
Feature change description .....	69
Command changes .....	69
Modified feature: Clearing IS-IS LSP log information .....	70
Feature change description .....	70
Command changes .....	70
Modified feature: Specifying a label allocation mode .....	70
Feature change description .....	70
Command changes .....	70
Modified command: <b>label-allocation-mode</b> .....	70
Modified feature: Displaying BGP peer or peer group information .....	71
Feature change description .....	71
Command changes .....	71
Modified command: display bgp peer .....	71
Modified feature: Displaying AS path information for BGP routes .....	71
Feature change description .....	71
Command changes .....	72
Modified feature: Displaying RPF information for an IPv6 multicast source ..	74
Feature change description .....	74
Command changes .....	74
Modified command: display ipv6 multicast rpf-info .....	74
Modified feature: Displaying statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping .....	75
Feature change description .....	75
Command changes .....	75
Modified command: display igmp-snooping statistics .....	75



Modified feature: Displaying statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping .....	77
Feature change description .....	77
Command changes .....	77
Modified command: display mld-snooping statistics .....	77
Modified feature: Enabling a VPN instance to replicate routes from the public network or other VPN instances .....	79
Feature change description .....	79
Command changes .....	79
Modified command: route-replicate .....	79
Modified feature: Specifying outgoing labels for a static SRLSP .....	79
Feature change description .....	79
Command changes .....	80
Modified command: static-sr-mpls lsp .....	80
Modified feature: Creating an ACL .....	80
Feature change description .....	80
Command changes .....	80
Modified command: acl .....	80
Modified feature: Referencing an ACL in QoS or packet filtering .....	81
Feature change description .....	81
Command changes .....	81
Modified command: none .....	81
Modified feature: Enabling hardware-count for the packet filtering default action .....	82
Feature change description .....	82
Command changes .....	82
Modified command: packet-filter default hardware-count .....	82
Modified feature: Configuring drop-level-based parameters for a queue in a WRED table .....	82
Feature change description .....	82
Command changes .....	83
Modified command: queue .....	83
Modified feature: Configuring binding attributes for a local user .....	83
Feature change description .....	83
Command changes .....	83
Modified command: bind-attribute .....	83
Modified feature: Password handling when global password control is enabled .....	84
Feature change description .....	84
Command changes .....	85
Modified feature: Setting the quiet timer for RADIUS servers .....	85
Feature change description .....	85
Command changes .....	85
Modified command: timer quiet (RADIUS scheme view) .....	85
Modified feature: Configuring MAC-based MAC authentication user accounts .....	85
Feature change description .....	85
Command changes .....	85

Modified command: mac-authentication user-name-format .....	85
<b>Modified feature: MAC authentication VLAN mode .....</b>	<b>86</b>
Feature change description .....	86
Command changes .....	86
Modified command: mac-authentication host-mode .....	86
<b>Modified feature: Port security MAC move .....</b>	<b>87</b>
Feature change description .....	87
Command changes .....	87
Modified command: port-security mac-move permit .....	87
<b>Modified feature: Web authentication support for HTTPS redirection .....</b>	<b>88</b>
<b>Modified feature: RSA key modulus length .....</b>	<b>88</b>
Feature change description .....	88
Command changes .....	88
Modified command: public-key local create .....	88
<b>Modified feature: RSA key modulus length used for certification request in a PKI domain .....</b>	<b>89</b>
Feature change description .....	89
Command changes .....	89
Modified command: public-key rsa .....	89
<b>Modified feature: Displaying IPv4SG bindings .....</b>	<b>89</b>
Feature change description .....	89
Command changes .....	90
Modified command: display ip source binding .....	90
<b>Modified feature: Displaying IPv6SG bindings .....</b>	<b>90</b>
Feature change description .....	90
Command changes .....	90
Modified command: display ipv6 source binding .....	90
<b>Modified feature: Displaying the MFF configuration for a VLAN .....</b>	<b>91</b>
Feature change description .....	91
Command changes .....	91
Modified command: display mac-forced-forwarding vlan .....	91
<b>Modified feature: Associating Track with application modules .....</b>	<b>92</b>
Feature change description .....	92
Command changes .....	92
Modified command: track bfd ctrl .....	92
Modified command: track bfd echo .....	93
Modified command: track cfd .....	93
Modified command: track interface .....	93
Modified command: track interface physical .....	94
Modified command: track interface protocol .....	94
Modified command: track ip route reachability .....	94
Modified command: track lldp neighbor .....	95
Modified command: track nqa .....	95
<b>Modified feature: Specifying the length of ICMP echo requests sent by an IPv4 or IPv6 ping operation .....</b>	<b>95</b>
Feature change description .....	95
Command changes .....	96
Modified command: ping .....	96
Modified command: ping ipv6 .....	96

Modified feature: Removing a TCP or UDP listening service for a VPN instance .....	96
Feature change description .....	96
Command changes .....	96
Modified command: nqa server tcp-connect .....	96
Modified command: nqa server udp-echo .....	97
Modified feature: Specifying the source IP address for NTP messages .....	97
Feature change description .....	97
Command changes .....	97
Modified command: ntp-service source .....	97
New feature: Specifying the NTP time-offset thresholds for log and trap outputs .....	98
Specifying the NTP time-offset thresholds for log and trap outputs .....	98
Command reference .....	98
ntp-service time-offset-threshold .....	98
New feature: Specifying the SNTP time-offset thresholds for log and trap outputs .....	99
Specifying the SNTP time-offset thresholds for log and trap outputs .....	99
Command reference .....	100
sntp time-offset-threshold .....	100
Modified feature: Creating a sampler .....	100
Feature change description .....	100
Command changes .....	101
Modified command: sampler .....	101
Modified feature: sFlow counter sampling .....	101
Feature change description .....	101
Command changes .....	101
Modified command: sflow counter collector .....	101
Modified feature: sFlow flow sampling .....	102
Feature change description .....	102
Command changes .....	102
Modified command: sflow counter collector .....	102
Modified feature: Configuring a backup PW for a cross-connect .....	102
Feature change description .....	102
Command changes .....	102
Modified command: backup-peer .....	102
Modified feature: Configuring a backup PW for a VSI .....	103
Feature change description .....	103
Command changes .....	103
Modified command: backup-peer .....	103
Modified feature: Change of the bandwidth limit value range for VSIs .....	103
Feature change description .....	103
Command changes .....	103
Modified command: <b>bandwidth</b> .....	103
Modified feature: Value range change for the broadcast, multicast, or unknown unicast restraint bandwidth of VSIs .....	104
Feature change description .....	104
Command changes .....	104
Modified command: <b>restrain</b> .....	104

Modified feature: Frame match criteria of VXLAN Ethernet service instances .....	104
Feature change description .....	104
Command changes .....	104
Modified command: encapsulation .....	104
Modified feature: Displaying EVPN routing table information.....	105
Feature change description .....	105
Command changes .....	105
Modified command: display evpn routing-table.....	105
Modified feature: NETCONF logging .....	106
Feature change description .....	106
Command changes .....	106
Modified command: netconf log .....	106
Modified feature: Specifying the role of the device in the VCF fabric.....	106
Feature change description .....	106
Command reference.....	107
Modified command: vcf-fabric role.....	107
Modified command: display vcf-fabric role.....	107
Modified command: display vcf-fabric underlay autoconfigure .....	108

# 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 5950-CMW710-F6207 (or earlier), see their respective release notes (software feature changes).

**Table 1 Software feature change summary**

Section	Software feature changes
Release 6301P02	Contains changes in HPE 5950-CMW710-R6301P02 over HPE 5950-CMW710-R6301P01.
Release 6301P01	Contains changes in HPE 5950-CMW710-R6301P01 over HPE 5950-CMW710-R6301.
Release 6301	Contains changes in HPE 5950-CMW710-R6301 over HPE 5950-CMW710-F6207.

# Release 6301P02

This release has no feature changes.

# Release 6301P01

This release has no feature changes.

# Release 6301

This release has the following changes:

- 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: MPLS 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: FC and FCoE features
- New features: OpenFlow features
- New features: VXLAN features
- New features: EVPN features
- Modified feature: ISSU by using issu commands
- Modified feature: Automatic configuration
- Modified feature: Setting the timestamp format for logs sent to log hosts
- 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: Displaying the operating status and information of an interface
- Modified feature: Displaying PFC information of all interfaces
- Modified feature: Link state change suppression on an interface
- Modified feature: MAC-to-VLAN entries
- Modified feature: Collision handling process of LACP MAD and BFD MAD
- Modified feature: Collision handling process of ND MAD
- Modified feature: Displaying global link aggregation load sharing modes
- Modified feature: Configuring a link aggregation load sharing hash seed
- Modified feature: Displaying detailed information about the IPP and DR interfaces of DRNI
- Modified feature: Configuring the advertisable TLVs for LLDP
- Modified feature: Setting the aging timer for dynamic ARP entries
- Modified feature: ARP snooping
- Modified feature: Specifying DHCP servers for a DHCP relay address pool
- Modified feature: Displaying DHCP snooping and DHCPv6 snooping trusted ports
- Modified feature: Displaying DHCP address pool information
- Modified feature: Displaying DHCPv6 address pool information
- Modified feature: Enabling recording DHCPv6 snooping address entries in VLAN view



- Modified feature: Setting the aging timer for ND entries in stale state
- Modified feature: Displaying member interfaces shut down by Monitor Link
- Modified feature: Displaying DLDAP configuration
- Modified feature: Configuring routing policy-based recursive lookup
- Modified feature: Associating Track with the output interface for a static route
- Modified feature: Configuring OSPF area authentication
- Modified feature: Configuring OSPF interface authentication
- Modified feature: Configuring a virtual link
- Modified feature: Setting the number of OSPF logs
- Modified feature: Displaying IS-IS LSP log information
- Modified feature: Clearing IS-IS LSP log information
- Modified feature: Specifying a label allocation mode
- Modified feature: Displaying BGP peer or peer group information
- Modified feature: Displaying AS path information for BGP routes
- Modified feature: Displaying RPF information for an IPv6 multicast source
- 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: Specifying outgoing labels for a static SRLSP
- Modified feature: Creating an ACL
- Modified feature: Referencing an ACL in QoS or packet filtering
- Modified feature: Enabling hardware-count for the packet filtering default action
- Modified feature: Configuring drop-level-based parameters for a queue in a WRED table
- Modified feature: Configuring binding attributes for a local user
- Modified feature: Password handling when global password control is enabled
- Modified feature: Setting the quiet timer for RADIUS servers
- Modified feature: Configuring MAC-based MAC authentication user accounts
- Modified feature: MAC authentication VLAN mode
- Modified feature: Port security MAC move
- Modified feature: Web authentication support for HTTPS redirection
- Modified feature: RSA key modulus length
- Modified feature: RSA key modulus length used for certification request in a PKI domain
- Modified feature: Displaying IPv4SG bindings
- Modified feature: Displaying IPv6SG bindings
- Modified feature: Displaying the MFF configuration for a VLAN
- Modified feature: Associating Track with application modules
- Modified feature: Specifying the length of ICMP echo requests sent by an IPv4 or IPv6 ping operation
- Modified feature: Removing a TCP or UDP listening service for a VPN instance
- Modified feature: Specifying the source IP address for NTP messages

- New feature: Specifying the NTP time-offset thresholds for log and trap outputs
- New feature: Specifying the SNTP time-offset thresholds for log and trap outputs
- Modified feature: Creating a sampler
- Modified feature: sFlow counter sampling
- Modified feature: sFlow flow sampling
- Modified feature: Configuring a backup PW for a cross-connect
- Modified feature: Configuring a backup PW for a VSI
- Modified feature: Change of the bandwidth limit value range for VSIs
- Modified feature: Value range change for the broadcast, multicast, or unknown unicast restraint bandwidth of VSIs
- Modified feature: Frame match criteria of VXLAN Ethernet service instances
- Modified feature: Displaying EVPN routing table information
- Modified feature: NETCONF logging
- Modified feature: Specifying the role of the device in the VCF fabric

## New features: Fundamentals features

Table 1 describes the fundamentals features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Fundamentals Configuration Guide* and *HPE FlexFabric 5950 Switch Series Fundamentals Command Reference*.

**Table 1 Fundamentals features added in version R6301**

Feature	Command changes
RBAC: Automatically obtaining the login username when a login user requests temporary user role authorization from a remote authentication server	The <b>super use-login-username</b> command was added.
Login management: Logging for Telnet login attempts that are denied by the Telnet login control ACL	The <b>telnet server acl-deny-log enable</b> command was added.
Login management: Setting the Telnet service port numbers	The following commands were added: <ul style="list-style-type: none"> <li>• <b>telnet server port</b> <i>port-number</i></li> <li>• <b>telnet server ipv6 port</b> <i>port-number</i></li> </ul>
FTP: Logging for FTP login attempts that are denied by the FTP login control ACL	The <b>ftp server acl-deny-log enable</b> command was added.
File system management: Executing a batch file	The <b>execute</b> <i>filename</i> command was added.
Configuration file management: Automatic system-wide next-startup configuration file operations	The <b>standby auto-update config</b> command was added.
Configuration file management: Archiving the running configuration to a remote SCP server	The following commands were added: <ul style="list-style-type: none"> <li>• <b>archive configuration server</b></li> <li>• <b>archive configuration server user</b></li> <li>• <b>archive configuration server password</b></li> </ul>
ISSU: Terminating the ongoing ISSU process forcibly	The <b>issu quit</b> command was added.

Feature	Command changes
Device management: Parity error alarm	The following commands were added: <ul style="list-style-type: none"> <li>• <b>parity-error monitor log enable</b></li> <li>• <b>parity-error monitor period</b></li> <li>• <b>parity-error monitor threshold</b></li> </ul>
Device management: Resource usage monitoring	The following commands were added: <ul style="list-style-type: none"> <li>• <b>resource-monitor minor resend enable</b></li> <li>• <b>resource-monitor output</b></li> <li>• <b>resource-monitor resource</b></li> </ul>
Device management: Setting the memory usage thresholds	The <b>ratio</b> , <b>early-warning</b> , and <b>secure</b> options were added to the <b>memory-threshold</b> command.
Device management: Displaying memory alarm thresholds and statistics	Early-warning threshold information was added to output from the <b>display memory-threshold</b> command.
Device management: Displaying the current CPU usage statistics	The <b>core</b> option was added to the <b>display cpu-usage</b> command.
Device management: Locating devices	The <b>locator blink</b> command was added.
Device management: Rebooting a subcard	The <b>subslot subslot-number</b> option was added to the <b>reboot</b> command.
Python: Comware extended Python API channel	N/A
Python: Comware extended Python API send	N/A
Python: Comware extended Python API SYSLOG	N/A
License management	All license management commands were newly added.

## New features: Virtual technologies features

[Table 2](#) describes the virtual technologies features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Virtual technologies Configuration Guide* and *HPE FlexFabric 5950 Switch Series Virtual technologies Command Reference*.

**Table 2 Virtual technologies features added in version R6301**

Feature	Command changes
Configuring ND MAD that uses management Ethernet ports	The <b>mad nd enable</b> command was added in management Ethernet interface view.

## New features: Layer 2—LAN switching features

[Table 3](#) describes the Layer 2—LAN switching features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Layer 2—LAN Switching Configuration Guide* and *HPE FlexFabric 5950 Switch Series Layer 2—LAN*

**Table 3 Layer 2—LAN switching features added in version R6301**

Feature	Command changes
Ethernet interfaces: Displaying the status and packet statistics of interfaces	The <b>display interface link-info</b> command was added.
Ethernet interfaces: Displaying operating status and information of all interfaces except subinterfaces	The <b>display interface main</b> command was added.
Ethernet interfaces: Configuring PFC on Ethernet interfaces	The following commands were added to system view: <ul style="list-style-type: none"> <li>• <b>priority-flow-control</b></li> <li>• <b>priority-flow-control no-drop dot1p</b></li> </ul>
Ethernet interfaces: Configuring PFC deadlock detection	The following commands were added: <ul style="list-style-type: none"> <li>• <b>priority-flow-control deadlock auto-recover action</b></li> <li>• <b>priority-flow-control deadlock auto-recover cos</b></li> <li>• <b>priority-flow-control deadlock threshold</b></li> </ul>
Ethernet interfaces: Enabling fast retrain.	The <b>port fast-retrain enable</b> command was added.
Ethernet interfaces: Setting the interface connection distance	The <b>port connection-distance</b> command was added.
Ethernet interfaces: Enabling link flapping protection on an interface	The following commands were added: <ul style="list-style-type: none"> <li>• <b>display link-flap protection</b></li> <li>• <b>link-flap protect enable</b></li> <li>• <b>port link-flap protect enable</b></li> </ul>
Ethernet link aggregation: Disabling the default port selection action for dynamic aggregation groups	The <b>lacp default-selected-port disable</b> command was added.
Ethernet link aggregation: Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection	The <b>lacp select speed</b> command was added.
Ethernet link aggregation: Setting a hash offset to adjust the load balancing hash results on link aggregations	The <b>link-aggregation global load-sharing offset</b> command was added.
Ethernet link aggregation: Setting the load sharing mode for tunneled traffic on link aggregations.	The <b>link-aggregation global load-sharing tunnel</b> command was added.
Ethernet link aggregation: Enabling an aggregation group to distribute traffic across the member links on a per-packet basis.	The <b>per-packet</b> keyword was added to the <b>link-aggregation load-sharing mode</b> command.
Ethernet link aggregation: Setting the minimum percentage of Selected ports in an aggregation group	The <b>percentage number</b> option was added to the <b>link-aggregation selected-port minimum</b> command.
Ethernet link aggregation: Setting the physical state change suppression interval on an	The <b>link-delay</b> command was added.

Feature	Command changes
aggregate interface	
VLAN mapping: Configuring two-to-one VLAN mapping	The <b>vlan mapping egress</b> command was added.
VLAN mapping: Configuring network-side many-to-one VLAN mapping	The <b>nni</b> keyword was added to the <b>vlan mapping</b> command.
DRNI: Enabling DR system auto-recovery and set the reload delay timer	The <b>drni auto-recovery reload-delay</b> command was added.
DRNI: Excluding an interface from the shutdown action by DRNI MAD	The <b>drni mad exclude interface</b> command was added.
Spanning tree: Enabling dispute guard	The <b>stp dispute-protection</b> command was added.
LLDP: Setting the timeout for receiving LLDP frames and enable the device to report no LLDP neighbor events	The <b>lldp timer rx-timeout</b> command was added.
LLDP: Enabling advertisement of the management address TLV globally and set the management address to be advertised	The <b>lldp global tlv-enable basic-tlv management-address-tlv</b> command was added.
LLDP: Clearing LLDP statistics on interfaces	The <b>reset lldp statistics</b> command was added.

## New features: Layer 3—IP services features

**Table 4** describes the Layer 3—IP services features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Layer 3—IP Services Configuration Guide* and *HPE FlexFabric 5950 Switch Series Layer 3—IP Services Command Reference*.

**Table 4 Layer 3—IP services features added in version R6301**

Feature	Command changes
ARP: Enabling interface consistency check between ARP and MAC address entries	The <b>arp mac-interface-consistency check enable</b> command was added.
ARP: Setting the maximum number of probes for dynamic ARP entries	The <b>arp timer aging probe-count</b> command was added.
ARP: Setting the interval for probing dynamic ARP entries	The <b>arp timer aging probe-interval</b> command was added.
ARP: Enabling recording user IP address conflicts	The <b>arp user-ip-conflict record enable</b> command was added.
ARP: Enabling recording user port migrations	The <b>arp user-move record enable</b> command was added.
ARP: Displaying user IP address conflict records	The <b>display arp user-ip-conflict record</b> command was added.
ARP: Displaying user port migration records	The <b>display arp user-move record</b> command was added.
ARP: Enabling ARP snooping in a VXLAN	The <b>arp snooping enable</b> command was added to VSI view.

Feature	Command changes
	<p>The <b>vsi</b> [<i>vsi-name</i>] option was added to the following commands:</p> <ul style="list-style-type: none"> <li><b>display arp snooping</b></li> <li><b>reset arp snooping</b></li> </ul>
ARP: Configuring a static ARP entry for a local site associated with the VXLAN gateway	<p>The <b>arp static ip-address mac-address vsi-interface vsi-interface-id interface-type interface-number service-instance instance-id vsi vsi-name [ vpn-instance vpn-instance-name ]</b> command was added.</p>
ARP: Setting the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change	<p>The <b>gratuitous-arp mac-change retransmit times interval seconds</b> command was added.</p>
DHCP server: Enabling the DHCP server to return a DHCP-NAK message if the client notions of their IP addresses are incorrect	<p>The <b>dhcp server request-ip-address check</b> command was added.</p>
DHCP: Binding the gateways to the DHCP server's MAC address in the address management module when the DHCP server assigns gateways to clients	<p>The <b>export-route</b> keyword was added to the <b>gateway-list</b> command.</p>
DHCP: Advertising the subnet assigned to DHCP clients when the DHCP server dynamically assigns IP addresses in the subnet to clients	<p>The <b>export-route</b> keyword was added to the <b>network</b> command.</p>
DHCP relay agent: Enabling the DHCP relay agent to insert Option 60 into DHCP requests	<p>The <b>dhcp relay insert option60</b> command was added.</p>
DHCP relay agent: Specifying a DHCP relay address pool for DHCP clients	<p>The <b>dhcp relay pool</b> command was added.</p>
DHCP snooping: Specifying the <b>append</b> handling strategy for Option 82 in request messages	<p>The <b>append</b> keyword was added to the <b>dhcp snooping information strategy</b> command.</p>
DHCP snooping: Configuring the padding mode for the Vendor-Specific sub-option	<p>The <b>dhcp snooping information vendor-specific</b> command was added.</p>
DHCP relay agent: Configuring the DHCP relay agent to perform a MAC address table lookup for a DHCP reply if it does not have the request forwarding information for the reply	<p>The <b>dhcp relay mac-forward enable [ broadcast ]</b> command was added.</p>
DHCP snooping: Enabling DHCP snooping for a VLAN	<p>The <b>dhcp snooping enable vlan</b> command was added.</p>
DHCP snooping: Enabling recording of client information in DHCP snooping entries for a VLAN	<p>The <b>dhcp snooping binding record</b> command was added to VLAN view.</p>
DHCP snooping: Disabling DHCP snooping on an interface	<p>The <b>dhcp snooping disable</b> command was added.</p>
DHCP snooping: Configuring an interface in a VLAN as a DHCP snooping trusted port	<p>The <b>dhcp snooping trust interface</b> command was added.</p>
IP forwarding basics: Enabling symmetric load sharing	<p>The <b>ip load-sharing symmetric enable</b> command was added.</p>

Feature	Command changes
IP addressing: Displaying IP configuration and statistics for interfaces of the specified interface type.	The <b>display ip interface <i>interface-type</i></b> command was added.
IP performance optimization: Enabling the device to encapsulate the TCP Timestamps option in outgoing TCP packets	The <b>tcp timestamps enable</b> command was added.
DNS: Enabling DNS proxy	The <b>dns proxy enable</b> command was added.
DNS: Enabling DNS spoofing and specifying the IPv4 address for spoofing DNS requests	The <b>dns spoofing ip-address [ vpn-instance <i>vpn-instance-name</i> ]</b> command was added.
DNS: Enabling DNS spoofing and specifying the IPv6 address for spoofing DNS requests	The <b>ipv6 dns spoofing ipv6-address [ vpn-instance <i>vpn-instance-name</i> ]</b> command was added.
IPv6 basics: Configuring ND snooping	<p>The following command were added:</p> <ul style="list-style-type: none"> <li><b>ipv6 nd snooping dad retrans-timer <i>interval</i></b></li> <li><b>ipv6 nd snooping enable global</b></li> <li><b>ipv6 nd snooping enable link-local</b></li> <li><b>ipv6 nd snooping glean source</b></li> <li><b>ipv6 nd snooping lifetime { invalid <i>invalid-lifetime</i>   valid <i>valid-lifetime</i> }</b></li> <li><b>ipv6 nd snooping max-learning-num <i>max-number</i></b></li> <li><b>ipv6 nd snooping uplink</b></li> <li><b>display ipv6 nd snooping</b></li> <li><b>display ipv6 nd snooping count</b></li> <li><b>reset ipv6 nd snooping [ [ vlan <i>vlan-id</i> ] [ global   link-local ]   vlan <i>vlan-id</i> ipv6-address ]</b></li> </ul>
IPv6 basics: Configuring ND snooping in a VXLAN	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li><b>ipv6 nd snooping enable global</b> (VSI view)</li> <li><b>ipv6 nd snooping enable link-local</b> (VSI view)</li> <li><b>display ipv6 nd snooping count vsi</b> (any view)</li> <li><b>display ipv6 nd snooping vsi</b> (any view)</li> <li><b>reset ipv6 nd snooping vsi</b> (user view)</li> </ul>
IPv6 basics: Enabling ND logging for user online and offline events	The <b>ipv6 nd online-offline-log enable</b> command was added.
IPv6 basics: Specifying the URL of the boot file in RA messages	The <b>ipv6 nd ra boot-file-url</b> command was added.
IPv6 basics: Specifying DNS suffix information to be advertised in RA messages	The <b>ipv6 nd ra dns search-list</b> command was added.
IPv6 basics: Enabling DNS suffix suppression	The <b>ipv6 nd ra dns search-list suppress</b>



Feature	Command changes
in RA messages	command was added.
IPv6 basics: Specifying DNS server information to be advertised in RA messages	The <b>ipv6 nd ra dns server</b> command was added.
IPv6 basics: Enabling DNS server suppression in RA messages	The <b>ipv6 nd ra dns server suppress</b> command was added.
IPv6 basics: Enabling ND direct route advertisement	The <b>ipv6 nd route-direct advertise</b> command was added.
IPv6 basics: Specifying a prefix length for generating a network route for identified ND entries	The <b>ipv6 nd route-direct prefix convert-length</b> command was added.
IPv6 basics: Recording user IPv6 address conflicts	The following commands were added: <ul style="list-style-type: none"> <li>• <b>ipv6 nd user-ip-conflict record enable</b></li> <li>• <b>display ipv6 nd user-ip-conflict record</b></li> </ul>
IPv6 basics: Recording user port migrations	The following commands were added: <ul style="list-style-type: none"> <li>• <b>ipv6 nd user-move record enable</b></li> <li>• <b>display ipv6 nd user-move record</b></li> </ul>
IPv6 basics: Setting the aging timer for ND entries in stale state on an interface	The <b>ipv6 neighbor timer stale-aging</b> command was added.
IPv6 basics: Enabling Layer 3 packet statistics counting	The <b>statistics l3-packet enable</b> command was added.
DHCPv6: Enabling IPv6 address binding conversion for IP source guard.	The <b>ipv6 dhcp server entry-convert enable</b> command was added.
DHCPv6: Advertising the subnet assigned to DHCPv6 clients when the DHCPv6 server dynamically assigns IPv6 addresses in the subnet to clients	The <b>export-route</b> keyword was added to the <b>network</b> command.
DHCPv6 relay agent: Enabling the DHCPv6 relay agent to advertise host routes for IPv6 addresses assigned to DHCP clients	The <b>ipv6 dhcp advertise address-route</b> command was added.
DHCPv6 relay agent: Enabling the DHCPv6 relay agent to support Option 79	The <b>ipv6 dhcp relay client-link-address enable</b> command was added.
DHCPv6 relay agent: Configuring the DHCPv6 relay agent to discard the DHCPv6 requests that are delivered from VXLAN tunnels	The <b>ipv6 dhcp relay request-from-tunnel discard</b> command was added.
DHCPv6 snooping: Disabling DHCP snooping	The <b>ipv6 dhcp snooping disable</b> command was added.
DHCPv6 snooping: Enabling DHCPv6 snooping for VLANs	The <b>ipv6 dhcp snooping enable vlan</b> command was added.
DHCPv6 snooping: Configuring a port in a VLAN as a DHCPv6 snooping trusted port	The <b>ipv6 dhcp snooping trust interface</b> command was added.
DHCPv6: Configuring DHCPv6 guard	The following commands were added: <ul style="list-style-type: none"> <li>• <b>device-role</b></li> </ul>



Feature	Command changes
	<ul style="list-style-type: none"> <li>• <code>display ipv6 dhcp guard policy</code></li> <li>• <code>if-match reply acl</code></li> <li>• <code>if-match server acl</code></li> <li>• <code>ipv6 dhcp guard apply policy</code></li> <li>• <code>ipv6 dhcp guard policy</code></li> <li>• <code>preference</code></li> <li>• <code>trust port</code></li> </ul>
DHCPv6: Enabling the EUI-64 address allocation mode	The <code>address-alloc-mode eui-64</code> command was added.
DHCPv6 snooping: Recording DHCPv6 snooping prefix entries	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li>• <code>ipv6 dhcp snooping pd binding record</code></li> <li>• <code>display ipv6 dhcp snooping pd binding</code></li> <li>• <code>reset ipv6 dhcp snooping pd binding</code></li> </ul>

## New features: Layer 3—IP routing features

Table 5 describes the Layer 3—IP routing features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Layer 3—IP Routing Configuration Guide* and *HPE FlexFabric 5950 Switch Series Layer 3—IP Routing Command Reference*.

**Table 5 Layer 3—IP routing features added in version R6301**

Feature	Command changes
IP routing basics: Clearing IPv4/IPv6 route statistics for all VPN instances or for the public network and all VPN instances	<p>The <code>all-routes</code> and <code>all-vpn-instance</code> keywords were added to the following commands:</p> <ul style="list-style-type: none"> <li>• <code>reset ip routing-table statistics protocol</code></li> <li>• <code>reset ipv6 routing-table statistics protocol</code></li> </ul>
IP routing basics: Displaying routing table information for all VPN instances or for the public network and all VPN instances	<p>The <code>all-routes</code> and <code>all-vpn-instance</code> keywords were added to the following commands:</p> <ul style="list-style-type: none"> <li>• <code>display ip routing-table</code></li> <li>• <code>display ipv6 routing-table</code></li> </ul>
IP routing basics: Enabling the RIB to flush route attribute information to the FIB	The <code>flush route-attribute</code> command was added.
IP routing basics: Setting the maximum number of active IPv4/IPv6 routes supported by the device.	The <code>routing-table limit</code> command was added.
Static routing: Specifying the index of the next hop when creating a static route.	The <code>nexthop-index index-string</code> option was added to the <code>ip route-static</code> command.
Static routing: Enabling periodic sending of ARP requests to the next hops of static routes.	The <code>ip route-static arp-request</code> command was added.

Feature	Command changes
OSPF: Displaying OSPF neighbor state change log information for the specified neighbor on the specified IRF member device.	The <i>neighbor-id</i> argument and <b>slot slot-number</b> option were added to the <b>display ospf event-log</b> command.
OSPF: Displaying information about the hello packets sent to or received from neighbors.	The <b>hello</b> keyword was added to the <b>display ospf peer</b> command.
OSPF: Displaying statistics for sent or received hello packets.	The <b>hello</b> keyword was added to the <b>display ospf statistics</b> command.
OSPF: Displaying log information about received or sent hello packets.	The <b>display ospf event-log hello</b> command was added.
OSPF: Displaying information about hello packets sent by OSPF interfaces.	The <b>display ospf interface hello</b> command was added.
OSPF: Enabling OSPF to limit the LSU transmit rate	The <b>ospf lsu-flood-control</b> command was added.
OSPF: Clearing OSPF neighbor state change information about an IRF member device.	The <b>slot</b> keyword was added to the <b>reset ospf event-log</b> command.
OSPF: Clearing OSPF log information about received or sent hello packets.	The <b>reset ospf event-log hello</b> command was added.
BGP: Specifying the period after reboot within which the startup policy is effective	The <b>bgp apply-policy on-startup duration</b> command was added.
BGP: Setting the MED attribute value in the startup policy	The <b>bgp policy on-startup med</b> command was added.
BGP: Enabling BGP to send withdrawal messages of the default route prior to other routes	The <b>default-route update-first</b> command was added.
BGP: Setting the BGP route sending rate	The <b>route-rate-limit</b> command was added.
BGP: Disabling BGP session establishment with all peers and peer groups	The <b>ignore all-peers</b> command was added.
BGP: Disabling BGP session establishment with a peer or peer group	The <b>graceful</b> , <b>community</b> , <b>local-preference</b> , and <b>med</b> keywords were added to the <b>peer ignore</b> command.
BGP: Setting the session retry timer	The following commands were added: <ul style="list-style-type: none"> <li><b>timer connect-retry</b></li> <li><b>peer timer connect-retry</b></li> </ul>
BGP: Disabling route recursion policy control for routes received from the specified peer or peer group	The <b>peer nexthop-recursive-policy disable</b> command was added.
BGP: BGP ORF capabilities negotiation	The following commands were added: <ul style="list-style-type: none"> <li><b>peer capability-advertise orf non-standard</b></li> <li><b>peer capability-advertise orf prefix-list</b></li> <li><b>display bgp peer received prefix-list</b></li> </ul>
BGP: BGP additional path feature	The following commands were added:

Feature	Command changes
	<ul style="list-style-type: none"> <li><b>additional-paths select-best</b></li> <li><b>peer additional-paths</b></li> <li><b>peer advertise additional-paths best</b></li> </ul> <p>The Add-Path related fields were added to the output from the following commands:</p> <ul style="list-style-type: none"> <li><b>display bgp routing-table ipv4 unicast</b></li> <li><b>display bgp routing-table ipv6 unicast</b></li> <li><b>display bgp routing-table vpnv4</b></li> <li><b>display bgp routing-table vpnv6</b></li> </ul>
BGP: BGP IPv4 RT filter related features	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li><b>address-family ipv4 rtfilter</b></li> <li><b>display bgp routing-table ipv4 rtfilter</b></li> </ul> <p>The <b>rtfilter</b> keyword was added to the following commands:</p> <ul style="list-style-type: none"> <li><b>display bgp group</b></li> <li><b>display bgp peer</b></li> <li><b>display bgp update-group</b></li> <li><b>refresh bgp</b></li> <li><b>reset bgp</b></li> </ul>
BGP: Configuring BGP features in BGP IPv4 RT filter address family view	<p>Support for BGP IPv4 RT filter address family view was added to the following commands:</p> <ul style="list-style-type: none"> <li><b>peer default-route-advertise</b></li> <li><b>peer enable</b></li> <li><b>peer reflect-client</b></li> <li><b>reflect between-clients</b></li> <li><b>reflector cluster-id</b></li> </ul>
BGP: Enabling BGP to prefer routes with an IPv6 next hop during optimal route selection	The <b>bestroute ipv6-nexthop</b> command was added.
BGP: Enabling BGP to ignore router IDs during optimal route selection.	The <b>bestroute router-id-ignore</b> command was added.
BGP: Enabling BGP to immediately send route updates for routes that match an IPv6 prefix list	The <b>bgp update-delay on-startup ipv6-prefix-list</b> command was added.
BGP: Specifying existent and nonexistent policies to control route advertisement	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li><b>peer advertise-policy exist-policy</b></li> <li><b>peer advertise-policy non-exist-policy</b></li> </ul>
BGP: Enabling BGP to ignore the first AS number of EBGp route updates received from a peer or peer group	The <b>peer ignore-first-as</b> command was added.
BGP: Enabling the route reflector to change the attributes of routes to be reflected	The <b>reflect change-path-attribute</b> command was added.
BGP: Configuring optimal route selection delay	The <b>route-select delay</b> command was added.

Feature	Command changes
BGP: Applying route update interval setting to withdrawn routes	The <b>route-update-interval withdrawn enable</b> command was added.
BGP: Configuring RPKI related features	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li>• <b>rpki</b></li> <li>• <b>server tcp</b></li> <li>• <b>port</b></li> <li>• <b>passwords</b></li> <li>• <b>refresh-time</b></li> <li>• <b>response-time</b></li> <li>• <b>purge-time</b></li> <li>• <b>check-origin-validation</b></li> <li>• <b>peer advertise origin-as-validation</b></li> <li>• <b>bestroute origin-as-validation</b></li> <li>• <b>reset bgp rpki server</b></li> <li>• <b>display bgp rpki server</b></li> <li>• <b>display bgp rpki table</b></li> </ul>
BGP: Configuring BGP BMP related features	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li>• <b>server connect-interface</b></li> <li>• <b>server vpn-instance</b></li> <li>• <b>route-mode adj-rib-out</b></li> <li>• <b>route-mode loc-rib</b></li> </ul>
BGP: Enabling BGP to send withdrawal messages of routes matching the specified routing policy prior to other routes	The <b>update-first route-policy</b> command was added.
BGP: Displaying BGP IPv4 unicast routes, IPv4 multicast routes, IPv6 unicast routes, and IPv6 multicast routes that match an AS path list specified by its name.	<p>The <i>as-path-acl-name</i> argument was added to the following commands:</p> <ul style="list-style-type: none"> <li>• <b>display bgp routing-table ipv4 unicast</b></li> <li>• <b>display bgp routing-table ipv4 multicast</b></li> <li>• <b>display bgp routing-table ipv6 unicast</b></li> <li>• <b>display bgp routing-table ipv6 multicast</b></li> </ul>
BGP: Displaying BGP update group information for IPv6 EVPN address family.	The <i>ipv6-address</i> argument was added to the <b>display bgp update-group l2vpn evpn</b> command.
BGP: Displaying BGP update group information for MVPN address family	The <b>mvpn</b> keyword was added to the <b>display bgp update-group ipv4</b> command.
BGP: Displaying route flap statistics for BGP routes that match an AS path list specified by its name.	The <i>as-path-acl-name</i> argument was added to the <b>display bgp routing-table flap-info</b> command.
BGP: Specifying an IPv4/IPv6 ACL by its name for the policy used to filter BGP routes.	<p>The <b>name</b> <i>ipv4-acl-name</i> and <b>name</b> <i>ipv6-acl-name</i> options were added to the following commands:</p> <ul style="list-style-type: none"> <li>• <b>filter-policy import</b></li> <li>• <b>filter-policy export</b></li> <li>• <b>peer filter-policy</b></li> </ul>

Feature	Command changes
BGP: Removing the specified routing policy applied to routes incoming from or outgoing to a peer or peer group	The <i>route-policy-name</i> argument was added to the <b>undo peer route-policy</b> command.
BGP: Removing an IPv6 prefix list specified to filter routes received from or advertised to a peer or peer group	The <i>ipv6-prefix-list-name</i> argument was added to the <b>undo peer prefix-list</b> command.
BGP: Redistributing the local network specified in the public instance or a VPN instance	The <b>import-route local-aggregate</b> command was added.
BGP: Specifying an AS path list by its name to filter routes incoming from or outgoing to a peer or peer group	The <i>as-path-acl-name</i> argument was added to the <b>peer as-path-acl</b> command.
BGP: Support for IPv6 BGP peers of specific commands	<p>The <i>ipv6-address prefix-length</i> argument was added to the following commands in BGP EVPN address family view:</p> <ul style="list-style-type: none"> <li>• <b>peer enable</b></li> <li>• <b>peer next-hop-local</b></li> <li>• <b>peer reflect-client</b></li> <li>• <b>peer route-policy</b></li> <li>• <b>peer advertise-community</b></li> <li>• <b>peer allow-as-loop</b></li> </ul>
BGP: Configuring BGP features in BGP MVPN address family view	<p>Support for BGP MVPN address family view was added to the following commands:</p> <ul style="list-style-type: none"> <li>• <b>peer reflect-client</b></li> <li>• <b>reflect between-clients</b></li> <li>• <b>reflector cluster-id</b></li> <li>• <b>refresh bgp</b></li> <li>• <b>reset bgp</b></li> </ul>
BGP: Displaying information about dynamic IPv6 peers or peer groups for the EVPN address family and resetting or soft resetting the BGP session to an IPv6 peer for the EVPN address family	<p>The <i>ipv6-address prefix-length</i> argument was added to the following commands:</p> <ul style="list-style-type: none"> <li>• <b>display bgp peer l2vpn evpn</b></li> <li>• <b>refresh bgp l2vpn evpn</b></li> <li>• <b>reset bgp l2vpn evpn</b></li> </ul>
BGP: Clearing flap statistics for BGP routes that match an AS path list specified by its name.	The <i>as-path-acl-name</i> argument was added to the <b>reset bgp flap-info</b> command.
Policy-based routing: Setting the action that drops matching packets when all next hops on a policy node are invalid	The <b>apply fail-action-drop next-hop</b> command was added.
Policy-based routing: Specifying NULL0 as the output interface for IP packets	The <b>apply output-interface NULL0</b> command was added.
Policy-based routing: Configuring a description for a policy node	The <b>description text</b> command was added.
Policy-based routing: Setting a local QoS ID match criterion for IP packets	The <b>qppb-manipulation</b> keyword was added to the <b>if-match qos-local-id</b> command.
IPv6 policy-based routing: Setting the action that drops matching IPv6 packets when all next hops on an IPv6 policy	The <b>apply fail-action-drop next-hop</b> command was added.

Feature	Command changes
node are invalid	
IPv6 policy-based routing: Specifying NULL0 as the output interface for IPv6 packets	The <b>apply output-interface NULL0</b> command was added.
IPv6 policy-based routing: Configuring a description for an IPv6 policy node	The <b>description text</b> command was added.
IPv6 policy-based routing: Setting a local QoS ID match criterion for IPv6 packets	The <b>qppb-manipulation</b> keyword was added to the <b>if-match qos-local-id</b> command.
Routing policy: Setting the SoO extended community attribute for BGP routes	The <b>apply extcommunity soo</b> command was added.
Routing policy: Matching BGP EVPN routes that have the specified L3VNI and setting an L3VNI for BGP EVPN routes	The following commands were added: <ul style="list-style-type: none"> <li><b>if-match l3-vni</b></li> <li><b>apply l3-vni</b></li> </ul>
Routing policy: Setting the BGP RPKI validation state match criterion	The <b>if-match rpki</b> command was added.
Routing policy: Configuring a route distinguisher (RD) list, matching routes whose RD matches the specified RD list, and displaying RD list information	The following commands were added: <ul style="list-style-type: none"> <li><b>ip rd-list</b></li> <li><b>if-match rd-list</b></li> <li><b>display ip rd-list</b></li> </ul>
Routing policy: Clearing BGP AS path list statistics	The <b>reset ip as-path</b> command was added.
Routing policy: Setting the routing policy change delay timer	The <b>route-policy-change delay-time</b> command was added.
Routing policy: Matching IPv6 prefixes with the specified length whose last bit is an even number.	The <b>if-match ipv6 even-prefix-length</b> command was added.
Routing policy: Matching IPv6 prefixes with the specified length whose last bit is an odd number.	The <b>if-match ipv6 odd-prefix-length</b> command was added.
Routing policy: Matching BGP routes whose AS_PATH attribute matches an AS path list specified by its name, configuring an AS path list and specifying its name, and displaying information about a BGP AS path list specified by its name.	The <i>as-path-name</i> argument was added to the following commands: <ul style="list-style-type: none"> <li><b>if-match as-path</b></li> <li><b>ip as-path</b></li> <li><b>display ip as-path</b></li> </ul>
Routing policy: Matching BGP EVPN IMET routes, BGP EVPN IP prefix advertisement routes, and BGP EVPN MAC/IP advertisement routes.	The <b>bgp-evpn-imet</b> , <b>bgp-evpn-ip-prefix</b> , and <b>bgp-evpn-mac-ip</b> keywords were added to the <b>if-match route-type</b> command.

## New features: IP multicast features

Table 6 describes IP multicast features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series IP Multicast Configuration Guide* and *HPE FlexFabric 5950 Switch Series IP Multicast Command Reference*.

**Table 6 IP multicast features added in version R6301**

Feature	Command changes
Setting the DSCP value in multicast protocol packets	The <b>dscp</b> command was added to IGMP snooping view, IGMP view, MSDP view, MLD snooping view, MLD view, and IPv6 PIM view.
IGMP snooping: Sending IGMP general queries upon a path change	The <b>send-query enable</b> command was added.
IGMP snooping: Displaying information about dynamic IGMP snooping group entries	The <b>display igmp-snooping group</b> command was added.
IGMP snooping: Enabling IGMP snooping querier election for a VLAN or VSI	The <b>igmp-snooping querier-election</b> command was added.
Multicast routing and forwarding: Mtrace	The following commands were added: <ul style="list-style-type: none"> <li>• <b>mtrace v1</b></li> <li>• <b>mtrace v2</b></li> <li>• <b>mtrace-service port</b></li> </ul>
Multicast routing and forwarding: Setting the maximum number of cached unknown multicast packets	The following commands were added: <ul style="list-style-type: none"> <li>• <b>multicast forwarding-table cache-unknown per-entry</b></li> <li>• <b>multicast forwarding-table cache-unknown total</b></li> </ul>
PIM: Display PIM routing entries for MVPN extranet	The <b>extranet { source-vpn-instance source-vpn-instance-name   source-public-instance   receive-vpn-instance receive-vpn-instance-name   receive-public-instance</b> option was added to the <b>display pim routing-table</b> command.
Multicast VPN: BGP IPv4 MVPN	The following commands were added: <ul style="list-style-type: none"> <li>• <b>address-family ipv4 mvpn</b></li> <li>• <b>display bgp routing-table ipv4 mvpn</b></li> <li>• <b>policy vpn-target</b></li> </ul>
Multicast VPN: Adding attributes Source AS Extended Community and RF Route Import Extended Community to routes that are sent to the BGP IPv4 MVPN neighbors	The <b>mvpn-advertise-rt-import</b> command was added.
Multicast VPN: Configuring an MVPN extranet RPF selection policy	The following commands were added: <ul style="list-style-type: none"> <li>• <b>multicast extranet select-rpf</b></li> <li>• <b>ipv6 multicast extranet select-rpf</b></li> </ul>
MLD snooping: Sending MLD general queries upon a path change	The <b>send-query enable</b> command was added.
MLD snooping: Displaying information about dynamic MLD snooping group entries	The <b>display mld-snooping group</b> command was added.
MLD snooping: Enabling MLD snooping querier election for a	The <b>mld-snooping querier-election</b> command was added.



Feature	Command changes
VLAN or VSI	
IPv6 multicast routing and forwarding: IPv6 mtrace	The following commands were added: <ul style="list-style-type: none"> <li><code>ipv6 mtrace-service port</code></li> <li><code>mtrace v2 ipv6</code></li> </ul>
IPv6 multicast routing and forwarding: Setting the maximum number of cached unknown IPv6 multicast packets	The following commands were added: <ul style="list-style-type: none"> <li><code>ipv6 multicast forwarding-table cache-unknown per-entry</code></li> <li><code>ipv6 multicast forwarding-table cache-unknown total</code></li> </ul>
IPv6 PIM: Embedded RP	The <code>embedded-rp</code> command was added.

## New features: MPLS features

[Table 7](#) describes the security features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series MPLS Configuration Guide* and *HPE FlexFabric 5950 Switch Series MPLS Command Reference*.

**Table 7 MPLS features added in version R6301**

Feature	Command changes
Basic MPLS: Displaying information about IS-IS SRLSPs	The <code>isis</code> keyword was added to the <code>display mpls lsp</code> command.
Static LSP: Displaying information about static LSPs deployed by OpenFlow	The <code>openflow</code> keyword is added to the <code>display mpls static-lsp</code> command.
MPLS TE: Setting the maximum link bandwidth and maximum reservable bandwidth in percentage for MPLS TE traffic	The <code>percent</code> parameters were added to the following commands: <ul style="list-style-type: none"> <li><code>mpls te max-link-bandwidth</code></li> <li><code>mpls te max-reservable-bandwidth</code></li> <li><code>mpls te max-reservable-bandwidth mam</code></li> <li><code>mpls te max-reservable-bandwidth rdm</code></li> </ul>
Tunnel policy: Displaying tunnel policy information	The <code>display tunnel-policy</code> command was added.
MPLS L3VPN: Specifying the local network to be advertised in the public instance or a VPN instance	The <code>network</code> command was added.
MPLS L3VPN: Replicating routes from a VPN instance to the public network	The <code>route-replicate from vpn-instance</code> command was added to public instance IPv4 address family view and public instance IPv6 address family view.
MPLS L3VPN: Creating an OSPF sham link with the None authentication mode	The <code>authentication-none</code> keyword was added to the <code>sham-link</code> command.
MPLS L3VPN: Enabling a VPN instance to replicate routes from the public network or other VPN instances	The <code>route-replicate</code> command was added to VPN instance IPv6 address family view.
MPLS L3VPN: Enabling ECMP VPN route redistribution	The <code>vpn-route cross multipath</code> command was added.
MPLS L2VPN: Configuring the	The <code>pw-redundancy</code> command was added.



Feature	Command changes
master/slave PW redundancy mode	
VPLS: Setting the maximum bandwidth for traffic on an AC	The <b>bandwidth</b> command was added to service instance view.
VPLS: Setting the expected bandwidth for a PW	The <b>bandwidth</b> command was added to VSI LDP PW view and VSI static PW view.
VPLS: Setting the maximum bandwidth for traffic in a VSI	The <b>bandwidth</b> command was added to VSI view.
VPLS: Configuring the master/slave PW redundancy mode	The <b>pw-redundancy</b> command was added.
MPLS OAM: PW connectivity verification	The following commands were added: <ul style="list-style-type: none"> <li>• <b>bfd discriminator</b></li> <li>• <b>display l2vpn pw bfd</b></li> <li>• <b>ping mpls pw</b></li> <li>• <b>vccv bfd</b></li> <li>• <b>vccv cc</b></li> </ul>
MPLS SR: Configuring an IS-IS prefix SID	The <b>isis prefix-sid</b> command was added.
MPLS SR: Enabling MPLS SR adjacency label allocation	The <b>segment-routing adjacency enable</b> command was added.
MPLS SR: Configuring the MPLS SRGB	The <b>segment-routing global-block</b> command was added.
MPLS SR: Enabling MPLS SR	The <b>segment-routing mpls</b> command was added.
MPLS SR: Configuring the device to prefer SRLSPs in traffic forwarding	The <b>segment-routing sr-prefer</b> command was added.
MPLS SR: Configuring a prefix segment for static MPLS SR	The <b>static-sr-mpls prefix</b> command was added.

## New features: ACL and QoS features

Table 8 describes the security features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series ACL and QoS Configuration Guide* and *HPE FlexFabric 5950 Switch Series ACL and QoS Command Reference*.

**Table 8 ACL and QoS features added in version R6301**

Feature	Command changes
ACL: Applying an ACL to a VLAN interface to filter packets	<p>The <b>packet-filter vlan-interface</b> command was added.</p> <p>The <b>vlan-interface</b> parameter was added to the following commands:</p> <ul style="list-style-type: none"> <li>• <b>display packet-filter statistics</b></li> <li>• <b>display packet-filter verbose</b></li> <li>• <b>reset acl counter</b></li> <li>• <b>reset packet-filter statistics</b></li> </ul>
ACL: Matching the local QoS ID in an advanced ACL rule	The <b>qos-local-id</b> parameter was added to the following

Feature	Command changes
	<p>commands:</p> <ul style="list-style-type: none"> <li><b>rule</b> (IPv4 advanced ACL view)</li> <li><b>rule</b> (IPv6 advanced ACL view)</li> </ul>
ACL: Matching VXLAN packets in a rule	<p>The following command was added to IPv4 advanced ACL view:</p> <ul style="list-style-type: none"> <li><b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } <b>vxlan</b> [ <b>destination</b> { <i>dest-address</i> <i>dest-wildcard</i>   <b>any</b> }   <b>source</b> { <i>source-address</i> <i>source-wildcard</i>   <b>any</b> }   <b>source-port</b> <i>operator</i> <i>port1</i> [ <i>port2</i> ]   <b>vxlan-id</b> <i>vxlan-id</i> ] * <b>inner-protocol</b> <i>inner-protocol</i> [ <b>counting</b>   <b>inner-destination</b> { <i>dest-address</i> <i>dest-wildcard</i>   <b>any</b> }   <b>inner-destination-port</b> <i>operator</i> <i>port1</i> [ <i>port2</i> ]   <b>inner-established</b>   <b>inner-source</b> { <i>source-address</i> <i>source-wildcard</i>   <b>any</b> }   <b>inner-source-port</b> <i>operator</i> <i>port1</i> [ <i>port2</i> ]   [ <b>logging</b> ]   <b>time-range</b> <i>time-range-name</i> ] *</li> </ul> <p>The following command was added to Layer 2 ACL view:</p> <ul style="list-style-type: none"> <li><b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } <b>vxlan</b> [ <b>counting</b>   <b>dest-mac</b> <i>dest-address</i> <i>dest-mask</i>   <b>inner-dest-mac</b> <i>inner-dest-address</i> <i>inner-dest-mask</i>   <b>inner-source-mac</b> <i>inner-source-address</i> <i>inner-source-mask</i>   <b>inner-type</b> <i>inner-protocol-type</i> <i>inner-protocol-type-mask</i>   <b>source-mac</b> <i>source-address</i> <i>source-mask</i>   <b>time-range</b> <i>time-range-name</i>   <b>type</b> <i>protocol-type</i> <i>protocol-type-mask</i>   <b>vxlan-id</b> <i>vxlan-id</i> ] *</li> </ul>
QoS: Matching the inner header information of VXLAN packets	The <b>inner</b> keyword was added to the <b>if-match acl</b> command.
QoS: Configuring a description for a traffic class	The <b>description</b> command was added.
QoS: Enabling MAC address learning for a traffic behavior	The <b>mac-address mac-learning enable</b> command was added.
QoS: Clearing queue-based outbound traffic statistics for interfaces	The <b>reset qos queue-statistics interface outbound</b> command was added.
QoS: Configuring trusting the 802.1p priority in the outer IP header of VXLAN packets	The <b>qos trust tunnel-dot1p</b> command was added.
QoS: Applying accounting-type QoS policies and marking-type QoS policies globally	<p>The <b>accounting</b> and <b>marking</b> keywords were added to the following commands:</p> <ul style="list-style-type: none"> <li><b>qos apply policy global</b></li> <li><b>display qos policy diagnosis global</b></li> <li><b>display qos policy global</b></li> <li><b>reset qos policy global</b></li> </ul>

## New features: Security features

Table 9 describes the security features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Security Configuration Guide* and *HPE FlexFabric 5950 Switch Series Security Command Reference*.

**Table 9 Security features added in version R6301**

Feature	Command changes
AAA: Configuring password control attributes for network access users	The following commands were added to network access users: <ul style="list-style-type: none"> <li><b>password-control length</b></li> <li><b>password-control complexity</b></li> <li><b>password-control composition</b></li> </ul>
AAA: Configuring an EAP profile	The following commands were added: <ul style="list-style-type: none"> <li><b>eap-profile</b></li> <li><b>method</b></li> <li><b>ca-file</b></li> </ul>
AAA: Support for EAP-based RADIUS server status detection	The <b>eap-profile</b> <i>eap-profile-name</i> option was added to the <b>radius-server test-profile</b> command.
AAA: Specifying a source interface for outgoing RADIUS packets	The <b>interface</b> <i>interface-type interface-number</i> option was added to the following commands: <ul style="list-style-type: none"> <li><b>radius nas-ip</b></li> <li><b>nas-ip</b> (RADIUS scheme view)</li> </ul>
AAA: Specifying a source interface for outgoing HWTACACS packets	The <b>interface</b> <i>interface-type interface-number</i> option was added to the following commands: <ul style="list-style-type: none"> <li><b>hwtacacs nas-ip</b></li> <li><b>nas-ip</b> (HWTACACS scheme view)</li> </ul>
AAA: Specifying a RADIUS server selection mode for reauthentication	The <b>reauthentication server-select</b> command was added.
AAA: Setting the version of RADIUS server status change MIB nodes	The <b>radius trap-version</b> command was added.
AAA: Disabling the RADIUS service	The [ <b>undo</b> ] <b>radius enable</b> command was added.
AAA: Displaying authentication and accounting load statistics for all RADIUS servers	The <b>display radius server-load statistics</b> command was added.
AAA: Clearing history authentication and accounting load statistics for all RADIUS servers	The <b>reset radius server-load statistics</b> command was added.
AAA: Configuring the AAA test feature	The following commands were added: <ul style="list-style-type: none"> <li><b>radius attribute-test-group</b></li> <li><b>include</b></li> <li><b>exclude</b></li> <li><b>test-aaa</b></li> </ul>
AAA: Configuring a connection recording policy	The following commands were added: <ul style="list-style-type: none"> <li><b>aaa connection-recording policy</b></li> <li><b>accounting hwtacacs-scheme</b></li> </ul>

Feature	Command changes
	<ul style="list-style-type: none"> <li><b>display aaa connection-recording policy</b></li> </ul>
AAA: Forcibly sending stop-accounting RADIUS packets	The <b>stop-accounting-packet send-force</b> command was added.
AAA: Specifying a RADIUS or HWTACACS server by its host name	<p>The <i>host-name</i> argument was added to the following commands:</p> <ul style="list-style-type: none"> <li><b>primary authentication</b> (RADIUS scheme view)</li> <li><b>primary accounting</b> (RADIUS scheme view)</li> <li><b>secondary authentication</b> (RADIUS scheme view)</li> <li><b>secondary accounting</b> (RADIUS scheme view)</li> <li><b>state secondary</b> (RADIUS scheme view)</li> <li><b>primary authentication</b> (HWTACACS scheme view)</li> <li><b>primary authorization</b> (HWTACACS scheme view)</li> <li><b>primary accounting</b> (HWTACACS scheme view)</li> <li><b>secondary accounting</b> (HWTACACS scheme view)</li> <li><b>secondary authorization</b> (HWTACACS scheme view)</li> <li><b>secondary authentication</b> (HWTACACS scheme view)</li> </ul>
AAA: Configuring a password in a test profile for detecting the RADIUS server status	The <b>password { cipher   simple } string</b> parameter was added to the <b>radius-server test-profile</b> command.
802.1X: Sending EAP-Success packets on assignment of users to the 802.1X Auth-Fail VLAN or VSI	The <b>dot1x auth-fail eapol</b> command was added.
802.1X: Configuring 802.1X unauthenticated user aging	<ul style="list-style-type: none"> <li>The <b>dot1x unauthenticated-user aging enable</b> command was added.</li> <li>The <b>user-aging { auth-fail-vlan   auth-fail-vsi   critical-vlan   critical-vsi   guest-vlan   guest-vsi } aging-time-value</b> parameters were added to the <b>dot1x timer</b> command.</li> </ul>
802.1X: Enabling 802.1X online user synchronization	The <b>dot1x server-recovery online-user-sync</b> command was added.
802.1X: Configuring 802.1X offline detection	<ul style="list-style-type: none"> <li>The <b>dot1x offline-detect enable</b> command was added.</li> <li>The <b>offline-detect offline-detect-value</b> option was added to the <b>dot1x timer</b> command.</li> </ul>
802.1X: Setting the maximum size of EAP-TLS fragments sent to the server	The <b>dot1x eap-tls-fragment to-server</b> command was added.
802.1X: Logging off 802.1X users	The <b>reset dot1x access-user</b> command was added.
802.1X: CAR attribute assignment	N/A
802.1X: Displaying the MAC addresses of 802.1X users in a type of 802.1X VLAN or VSI.	The <b>display dot1x mac-address</b> command was added.
802.1X: Enabling 802.1X user logging	The <b>dot1x access-user log enable</b> command was added.

Feature	Command changes
802.1X: Configuring 802.1X MAC address binding	The following commands were added: <ul style="list-style-type: none"> <li><b>dot1x mac-binding</b></li> <li><b>dot1x mac-binding enable</b></li> </ul>
802.1X: Support for VSI manipulation	The following commands were added: <ul style="list-style-type: none"> <li><b>dot1x auth-fail vsi</b></li> <li><b>dot1x critical vsi</b></li> <li><b>dot1x guest-vsi</b></li> <li><b>dot1x guest-vsi-delay</b></li> <li><b>reset dot1x guest-vsi</b></li> </ul>
802.1X: Configuring 802.1X on Layer 2 aggregate interfaces	The following commands were added to Layer 2 aggregate interface view: <ul style="list-style-type: none"> <li><b>dot1x</b></li> <li><b>dot1x auth-fail vsi</b></li> <li><b>dot1x critical vsi</b></li> <li><b>dot1x guest-vsi</b></li> <li><b>dot1x max-user</b></li> </ul>
MAC authentication: Specifying an authentication method for MAC authentication	The <b>mac-authentication authentication-method</b> command was added.
MAC authentication: Configuring user aging for unauthenticated MAC authentication users	<ul style="list-style-type: none"> <li>The <b>mac-authentication unauthenticated-user aging enable</b> command was added.</li> <li>The <b>user-aging { critical-vlan   critical-vsi   guest-vlan   guest-vsi } aging-time-value</b> parameters were added to the <b>mac-authentication timer</b> command in system view.</li> </ul>
MAC authentication: Configuring MAC authentication offline detection for a MAC authentication user	The <b>mac-authentication offline-detect mac-address</b> command was added.
MAC authentication: Enabling online user synchronization for MAC authentication	The <b>mac-authentication server-recovery online-user-sync</b> command was added.
MAC authentication: Specifying an ACL-based filter to identify source IP addresses that can or cannot trigger MAC authentication	The <b>exclude-ip acl acl-number</b> option was added to the <b>mac-authentication carry user-ip</b> command.
MAC authentication: Logging off MAC authentication users	The <b>reset mac-authentication access-user</b> command was added.
MAC authentication: CAR attribute assignment	N/A
MAC authentication: Displaying the MAC addresses of MAC authentication users in a type of MAC authentication VLAN or VSI.	The <b>display mac-authentication mac-address</b> command was added.
MAC authentication: Enabling MAC authentication user logging	The <b>mac-authentication access-user log enable</b> command was added.
MAC authentication: Support for VSI	The following commands were added:

Feature	Command changes
manipulation	<ul style="list-style-type: none"> <li><code>mac-authentication critical vsi</code></li> <li><code>mac-authentication guest-vsi</code></li> <li><code>mac-authentication guest-vsi auth-period</code></li> <li><code>reset mac-authentication critical vsi</code></li> <li><code>reset mac-authentication guest-vsi</code></li> </ul>
MAC authentication: Configuring MAC authentication on Layer 2 aggregate interfaces	<p>The following commands were added to Layer 2 aggregate interface view:</p> <ul style="list-style-type: none"> <li><code>mac-authentication</code></li> <li><code>mac-authentication critical vsi</code></li> <li><code>mac-authentication guest-vsi</code></li> <li><code>mac-authentication guest-vsi auth-period</code></li> <li><code>mac-authentication max-user</code></li> </ul>
Portal: Enabling the device to check the issuing of category-2 portal filtering rules	The <code>portal user-rule assign-check enable</code> command was added.
Portal: Configuring the NAS-Port-Type attribute carried in outgoing RADIUS requests	The <code>portal nas-port-type</code> command was added.
Portal: Support for Web proxy	The <code>portal web-proxy port</code> command was added.
Web authentication	All Web authentication commands were newly added.
Triple authentication	N/A
Port security: Support for ntkauto mode of the need to known (NTK) feature	The <code>ntkauto</code> keyword was added to the <code>port-security ntk-mode</code> command.
Port security: Setting the block timer for blocked MAC addresses	The <code>port-security timer blockmac</code> command was added.
Port security: Logging the first access attempt from a new MAC address in a VLAN after port security's MAC address limit for that VLAN is reached	The <code>vlan-mac-limit</code> keyword was added to the <code>port-security access-user log enable</code> command.
Port security: Enabling port security user logging	The <code>port-security access-user log enable</code> command was added.
Port security: Enabling the quiet timer for 802.1X or MAC authentication users that are logged off by the authorization-fail-offline feature	The <code>quiet-period</code> keyword was added to the <code>port-security authorization-fail offline</code> command.
Port security: Setting port security's limit on the number of MAC addresses for specific VLANs on a port	The <code>port-security mac-limit</code> command was added.
Port security: Setting the secure MAC aging timer in seconds	The <code>second</code> keyword was added to the <code>port-security timer autolearn aging</code> command.
Port security: Configuring the escape critical VSI feature	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li><code>port-security global escape critical-vsi</code></li> <li><code>port-security escape critical-vsi</code></li> </ul>
Password control: Setting the user authentication timeout time	The <code>password-control authentication-timeout</code> command was added.
Password control: Enabling the	The <code>password-control change-password</code>

Feature	Command changes
password change at first login feature	<b>first-login enable</b> command was added.
Password control: Enabling password control globally for network access users	The <b>network-class</b> keyword was added to the <b>password-control enable</b> command.
Password control: Deleting history password records for network access users	The <b>network-class [ user-name user-name ]</b> parameters were added to the <b>reset password-control history-record</b> command.
IPsec: Specifying the ECDSA signature authentication method for an IKE proposal	The <b>ecdsa-signature</b> keyword was added to the <b>authentication-method</b> command.
IPsec: Specifying the DH group <b>group19</b> , <b>group20</b> , or <b>group24</b> to be used for key negotiation in IKE phase 1	<ul style="list-style-type: none"> <li>In non-FIPS mode, the <b>group19</b> and <b>group20</b> keywords were added to the <b>dh</b> command.</li> <li>In FIPS mode, the <b>group19</b>, <b>group20</b>, and <b>group24</b> keywords were added to the <b>dh</b> command.</li> </ul>
SSH: Specifying keyboard-interactive authentication	The <b>keyboard-interactive</b> keyword was added to the <b>ssh user</b> command.
SSH: Support for non-interactive method to connect to the SCP server	The <b>no-more-input</b> keyword was added to the <b>scp</b> and <b>scp ipv6</b> commands.
SSH: Disconnecting SSH sessions	The <b>free ssh { user-ip { ip-address   ipv6 ipv6-address } [ port port-number ]   user-pid pid-number   username username }</b> command was added.
SSH: Logging for SSH login attempts that are denied by the SSH login control ACL	The <b>ssh server acl-deny-log enable</b> command was added.
SSH: Enabling SSH algorithm renegotiation and key re-exchange	The <b>ssh server key-re-exchange enable</b> command was added.
SSH: Specifying the SSH service port	The <b>ssh server port</b> command was added.
SSH: Deleting server public keys saved in the public key file on the Stelnet client	The <b>delete ssh client server-public-key</b> command was added.
SSH: Displaying server public key information saved in the public key file on the SSH client	The <b>display ssh client server-public-key</b> command was added.
SSH: Specifying and displaying the source IP address for outgoing SCP packets	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li><b>display scp client source</b></li> <li><b>scp client source</b></li> <li><b>scp client ipv6 source</b></li> </ul>
SSL: Enabling the SSL server to send the complete certificate chain to the client during SSL negotiation	The <b>certificate-chain-sending enable</b> command was added.
Attack detection and prevention: Applying an attack defense policy to an interface	The <b>attack-defense apply policy</b> command was added.
Attack detection and prevention: Enabling the blacklist feature on an interface	The <b>blacklist enable</b> command was added.



Feature	Command changes
IP source guard: Displaying IPv6SG prefix bindings	The <b>display ipv6 source binding pd</b> command was added.
ARP attack protection: Enabling logging for source MAC-based ARP attack detection	The <b>arp source-mac log enable</b> command was added.
ARP attack protection: Support for specifying an IRF member device if the specified interface is a virtual interface when displaying ARP attack entries detected by source MAC-based ARP attack detection	The <b>slot slot-number</b> option can be specified following the <b>interface interface-type interface-number</b> option in the <b>display arp source-mac</b> command if the specified interface is a virtual interface.
ARP attack protection: Specifying the maximum number of ARP attack detection logs for each log output	The <b>number number</b> option was added to the <b>arp detection log enable</b> command.
ARP attack protection: Specifying the rate at which the device sends ARP requests for ARP scanning	The <b>send-rate pps</b> option was added to the <b>arp scan</b> command.
ARP attack protection: Setting the interval for sending ARP detection logs to the information center	The <b>interval interval</b> option was added to the <b>arp detection log enable</b> command.
ND attack defense: Enabling ND attack detection logging	The <b>ipv6 nd detection log enable</b> command was added.
ND attack defense: ND attack detection	The following commands were added: <ul style="list-style-type: none"> <li>• <b>ipv6 nd detection enable</b></li> <li>• <b>ipv6 nd detection trust</b></li> <li>• <b>display ipv6 nd detection statistics</b></li> <li>• <b>reset ipv6 nd detection statistics</b></li> </ul>
MFF	All MFF commands were newly added.
MACsec: Setting the MKA life time	The <b>mka timer mka-life</b> command was added.

## New features: High availability features

Table 10 describes the high availability features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series High Availability Configuration Guide* and *HPE FlexFabric 5950 Switch Series High Availability Command Reference*.

**Table 10 High availability features added in version R6301**

Feature	Command changes
RRPP: Setting the link-up delay timer	The <b>linkup-delay-timer</b> command was added.
DLDP: Enabling DLDP on a port	The <b>initial-unidirectional-delay</b> keyword was added to the <b>dldp enable</b> command.
BFD: Configuring the BFD authentication mode for single-hop BFD control packets	The <b>hmac-md5</b> , <b>hmac-mmd5</b> , <b>hmac-msha1</b> , and <b>hmac-sha1</b> keywords were added to the <b>bfd authentication-mode</b> command.
BFD: Configuring BFD session flapping suppression	The <b>bfd dampening</b> command was added.



Feature	Command changes
BFD: Creating a BFD session for detecting the local interface state	The <b>template</b> <i>template-name</i> option was added to the <b>bfd detect-interface source-ip</b> command.
BFD: Configuring the timer that delays reporting the first BFD session establishment failure to the data link layer	The <b>bfd detect-interface first-fail-timer</b> command was added.
BFD: Enabling special processing for BFD sessions	The <b>bfd detect-interface special-processing</b> command was added.
BFD: Configuring the authentication mode for multihop BFD control packets	The <b>hmac-md5</b> , <b>hmac-mmd5</b> , <b>hmac-msha1</b> , and <b>hmac-sha1</b> keywords were added to the <b>bfd multi-hop authentication-mode</b> command.
BFD: Setting the local discriminator for the reflector	The <b>sbfd local-discriminator</b> command was added.
BFD: Displaying SBFD session information	The <b>display sbfd session</b> command was added.
VRRP: Specifying IPv4 VRRP control VLANs.	The <b>vrrp dot1q</b> command was added.
VRRP: Specifying IPv6 VRRP control VLANs	The <b>vrrp ipv6 dot1q</b> command was added.
VRRP: Specifying IPv4 VRRP control VLANs in 25GE interface view	Support for 25GE interface view was added to the <b>vrrp dot1q</b> command.
VRRP: Specifying IPv6 VRRP control VLANs in 25GE interface view	Support for 25GE interface view was added to the <b>vrrp ipv6 dot1q</b> command.
Track: Creating a track entry and associating it with the neighbor availability status of an LLDP interface	The <b>track lldp neighbor</b> command was added.
Track: Configuring a tracked list.	<p>The following commands were added:</p> <ul style="list-style-type: none"> <li>• <b>delay</b></li> <li>• <b>object</b></li> <li>• <b>threshold percentage</b></li> <li>• <b>threshold weight</b></li> <li>• <b>track list boolean</b></li> <li>• <b>track list threshold percentage</b></li> <li>• <b>track list threshold weight</b></li> </ul>

## New features: Network management and monitoring features

**Table 11** describes the network management and monitoring features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series Network Management and Monitoring Configuration Guide* and *HPE FlexFabric 5950 Switch Series Network Management and Monitoring Command Reference*.

**Table 11 Network management and monitoring features added in R6301**

Feature	Command changes
Information center: Displaying information about log output filters.	The <b>display info-center filter</b> command was added.
Information center: Displaying the content of the log file buffer.	The <b>display logfile buffer</b> command was added.
Information center: Displaying the content of the security log file buffer.	The <b>display security-logfile buffer</b> command was added.
Information center: Creating a log output filter.	The <b>info-center filter</b> <i>filter-name</i> { <b>module-name</b>   <b>default</b> } { <b>deny</b>   <b>level severity</b> } command was added.
Information center: Specifying a log host and configuring output parameters.	The <b>filter</b> <i>filter-name</i> option was added to the <b>info-center loghost</b> command.
Information center: Displaying log buffer information and buffered logs.	The <b>last-mins</b> <i>mins</i> option was added to the <b>display logbuffer</b> command.
Information center: Specifying a log host and to configure output parameters.	The <b>dscp</b> <i>dscp-value</i> option was added to the <b>info-center loghost</b> [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] { <i>hostname</i>   <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } [ <b>port</b> <i>port-number</i> ] [ <b>dscp</b> <i>dscp-value</i> ] [ <b>facility</b> <i>local-number</i> ] command.
SNMP: Creating an SNMP community, group, or user.	Support for specifying an advanced ACL was added to the following commands: <ul style="list-style-type: none"> <li><b>snmp-agent community</b></li> <li><b>snmp-agent group</b></li> <li><b>snmp-agent usm-user</b> { <b>v1</b>   <b>v2c</b> }</li> <li><b>snmp-agent usm-user v3</b></li> </ul>
SNMP: Setting the DSCP priority for SNMP responses.	The <b>snmp-agent packet response dscp</b> command was added.
SNMP: Configuring an SNMP notification target host.	The <b>dscp</b> <i>dscp-value</i> option was added to the following commands: In non-FIPS mode: <b>snmp-agent target-host trap address</b> <b>udp-domain</b> { <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } [ <b>udp-port</b> <i>port-number</i> ] [ <b>dscp</b> <i>dscp-value</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] <b>params</b> <b>securityname</b> <i>security-string</i> [ <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>authentication</b>   <b>privacy</b> ] ] In FIPS mode: <b>snmp-agent target-host trap address</b> <b>udp-domain</b> { <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } [ <b>udp-port</b> <i>port-number</i> ] [ <b>dscp</b> <i>dscp-value</i> ] [ <b>vpn-instance</b> <i>vpn-instance-name</i> ] <b>params securityname</b> <i>security-string</i> <b>v3</b> { <b>authentication</b>   <b>privacy</b> } 
EAA: Adding a reboot action to a monitor policy.	The <b>subslot</b> keyword was added to the <b>action reboot</b> command.

Feature	Command changes
Ansible	N/A
NETCONF: Specifying the <b>error-when-rollback</b> attribute in the <Configuration> element.	N/A
NETCONF: Configuring the device to use module-specific namespaces.	The <b>netconf capability specific-namespace</b> command was added.

## New features: FC and FCoE features

Table 12 describes the security features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series FC and FCoE Configuration Guide* and *HPE FlexFabric 5950 Switch Series FC and FCoE Command Reference*.

**Table 12 FC and FCoE features added in version R6301**

Feature	Command changes
Enabling area ID-to-F_Port binding	The following commands were added: <ul style="list-style-type: none"> <li><b>fc port-bind-area enable</b></li> <li><b>display fc port-bind-area [ vsan vsan-id ]</b></li> </ul>
Enabling BB_Credit recovery for an FC interface	The <b>fc b2bcredit recovery enable</b> command was added. The following information was added to the <b>display interface fc</b> command output: <ul style="list-style-type: none"> <li>BB_Credit Recovery is enabled.</li> <li>BB_Credit Recovery is disabled.</li> </ul>

## New features: OpenFlow features

Table 13 describes OpenFlow features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series OpenFlow Configuration Guide* and *HPE FlexFabric 5950 Switch Series OpenFlow Command Reference*.

**Table 13 OpenFlow features added in version R6301**

Feature	Command changes
Configuring an MPLS flow table for an OpenFlow instance	The <b>mpls</b> keyword was added to the <b>flow-table</b> command.
Configuring controllers to which ARP packets are forbidden to be reported	The <b>forbidden packet-in arp controller</b> command was added.
Excluding the specified VLANs from the VLANs in which traffic is forwarded in the OpenFlow forwarding process	The <b>openflow normal-forward vlan</b> command was added.

## New features: VXLAN features

Table 14 describes the VXLAN features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series VXLAN Configuration Guide* and *HPE FlexFabric 5950 Switch Series VXLAN Command Reference*.

**Table 14 VXLAN features added in version R6301**

Feature	Command changes
Displaying ND flood suppression entries	The <b>display ipv6 nd suppression vsi</b> command was added.
Disabling flooding for a VSI	The <b>all-direction</b> and <b>dci</b> keywords were added to the <b>flooding disable</b> command.
Enabling ND flood suppression	The <b>ipv6 nd suppression enable</b> command was added.
Clearing ND flood suppression entries on VSIs	The <b>reset ipv6 nd suppression vsi</b> command was added.
Configuring the VLAN tag processing rule for incoming traffic	The <b>rewrite inbound tag</b> command was added.
Configuring the VLAN tag processing rule for outgoing traffic	The <b>rewrite outbound tag</b> command was added.
Enabling packet statistics for a manually created VXLAN or VXLAN-DCI tunnel	The <b>statistics enable</b> command was added in tunnel interface view.
Enabling packet statistics for automatically created VXLAN tunnels	The <b>tunnel statistics vxlan auto</b> command was added.
Disabling the ACLs issued by the OVSDB controller	The <b>vtep acl disable</b> command was added.
Disabling remote ND learning for VXLANs	The <b>vxlan tunnel nd-learning disable</b> command was added.
Configuring VLAN-based VXLAN assignment	The <b>vxlan vlan-based</b> and <b>vxlan vni</b> commands were added.
Enabling packet statistics for Ethernet service instances of a VLAN	The <b>ac statistics enable</b> command was added.
Assigning backup VXLAN tunnels to a VXLAN	The <b>tunnel</b> command has the following changes: <ul style="list-style-type: none"> <li>The <b>backup-tunnel</b> keyword was added.</li> <li>The <b>remote-vni</b> keyword was removed.</li> </ul>
Displaying detailed information about MAC address entries for VSIs	The <b>verbose</b> keyword was added to the <b>display l2vpn mac-address</b> command.
Testing the reachability of a remote VM	The following commands were added: <ul style="list-style-type: none"> <li><b>emulate-ping vxlan</b></li> <li><b>emulate-ping vxlan enable</b></li> </ul>

## New features: EVPN features

Table 15 describes the EVPN features added in this software version. For more information about the features and commands, see *HPE FlexFabric 5950 Switch Series EVPN Configuration Guide*

**Table 15 EVPN features added in version R6301**

Feature	Command changes
Enabling BGP EVPN route advertisement for the BGP VPNv4 or VPNv6 address family	The <b>advertise evpn route</b> command was added.
Enabling BGP VPNv4 or VPNv6 route advertisement for the BGP EVPN address family	The <b>advertise l3vpn route</b> command was added.
Disabling ARP information advertisement for an EVPN instance	The <b>arp-advertising disable</b> command was added.
Displaying information about IPv4 peers that are automatically discovered through MAC/IP advertisement routes	The <b>mac-ip</b> keyword was added to the <b>display evpn auto-discovery</b> command.
Displaying EVPN ND flood suppression entries	The <b>display evpn route nd suppression</b> command was added.
Specifying the IP addresses of the VTEPs in a DR system	The <b>evpn drni local</b> command was added.
Configuring the EVPN global MAC address	The <b>evpn global-mac</b> command was added.
Enabling the device to redistribute received MAC/IP advertisement routes that contain ARP or ND information into a BGP unicast routing table	The <b>import evpn mac-ip</b> command was added.
Disabling generation of IP prefix advertisement routes for the subnets of a VSI interface	The <b>ip-prefix-route generate disable</b> command was added.
Enabling conversational learning for remote MAC address entries	The <b>mac-address forwarding-conversational-learning</b> command was added.
Disabling an EVPN instance from learning MAC addresses from ND information	The <b>nd mac-learning disable</b> command was added.
Suppressing the advertisement of specific BGP EVPN routes to a peer or peer group	The <b>peer advertise evpn-route suppress</b> command was added.
Replacing the L3 VXLAN ID and RD of IP prefix advertisement routes	The <b>peer re-originated</b> command was added.
Automatically generating an RD based on the router ID	The <b>router-id</b> keyword was added to the <b>route-distinguisher</b> command.

## Modified feature: ISSU by using issu commands

### Feature change description

You can use **issu** commands to display or install patch images.

# Command changes

## Modified command: display version comp-matrix

### Old syntax

```
display version comp-matrix file { boot filename | system filename |  
feature filename&<1-30> } *  
  
display version comp-matrix file ipe ipe-filename
```

### New syntax

```
display version comp-matrix file { boot filename | system filename |  
feature filename&<1-30> | patch filename&<1-30> } *  
  
display version comp-matrix file ipe ipe-filename [ patch  
filename&<1-30> ]
```

### Views

Any view

### Parameters

**patch:** Specifies a space-separated list of up to 30 patch image files.

**filename:** Specifies a .bin file in the *filesystemname/filename.bin* format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

### Change description

Before modification: The command does not support patch image files.

After modification: The command supports patch image files.

## Modified command: issu load

### Old syntax

```
issu load file { boot filename | system filename | feature filename&<1-30> }  
* slot slot-number&<1-9> [ reboot ]  
  
issu load file ipe ipe-filename slot slot-number&<1-9> [ reboot ]
```

### New syntax

```
issu load file { boot filename | system filename | feature filename&<1-30>  
| patch filename&<1-30> } * slot slot-number&<1-9> [ reboot ]  
  
issu load file ipe ipe-filename [ patch filename&<1-30> ] slot  
slot-number&<1-9> [ reboot ]
```

### Views

User view

### Parameters

**patch:** Specifies a space-separated list of up to 30 patch image files.

**filename:** Specifies a .bin file in the *filesystemname/filename.bin* format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

## Change description

Before modification: The command does not support patch image files.

After modification: The command supports patch image files.

## Modified command: `issu one-step`

### Old syntax

```
issu one-step file { boot filename | system filename | feature filename&<1-30> } * [ slot slot-number&<1-9> ] [ reboot ]
```

```
issu one-step file ipe ipe-filename slot slot-number&<1-9> [ reboot ]
```

### New syntax

```
issu one-step file { boot filename | system filename | feature filename&<1-30> | patch filename&<1-30> } * [ slot slot-number&<1-9> ] [ reboot ]
```

```
issu one-step file ipe ipe-filename [ patch filename&<1-30> ] slot slot-number&<1-9> [ reboot ]
```

### Views

User view

### Parameters

**patch**: Specifies a space-separated list of up to 30 patch image files.

*filename*: Specifies a .bin file in the *filesystemname/filename.bin* format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide*.

## Change description

Before modification: The command does not support patch image files.

After modification: The command supports patch image files.

## Modified feature: Automatic configuration

### Feature change description

Before modification: The device supports automatic configuration only on IPv4 networks.

After modification: The device supports automatic configuration on both IPv4 and IPv6 networks.

### Command changes

None

## Modified feature: Setting the timestamp format for logs sent to log hosts

### Feature change description

From this release, the timestamp for logs output to log hosts can be accurate to milliseconds.

### Command changes

#### Modified command: info-center timestamp loghost

##### Old syntax

```
info-center timestamp loghost { date | iso [ with-timezone ] | no-year-date | none }  
  
undo info-center timestamp loghost
```

##### New syntax

```
info-center timestamp loghost { date [ with-milliseconds ] | iso [ with-milliseconds | with-timezone ] * | no-year-date | none }  
  
undo info-center timestamp loghost
```

##### Change description

Before modification: The log timestamp cannot be accurate to milliseconds.

After modification: The log timestamp can be set to be accurate to milliseconds. The millisecond value is appended to the time information in the timestamp with a dot as the separator.

## Modified feature: Configuring an interface event for a CLI-defined EAA monitor policy

### Feature change description

This release added support of monitoring traffic statistics on multiple interfaces. The interfaces in an interface range must be the same type.

### Command changes

#### Modified command: event-interface

##### Old syntax

```
event interface interface-type interface-number monitor-obj monitor-obj  
start-op start-op start-val start-val restart-op restart-op restart-val  
restart-val [ interval interval ]
```

##### New syntax

```
event interface interface-list monitor-obj monitor-obj start-op start-op  
start-val start-val restart-op restart-op restart-val restart-val  
[ interval interval ]
```



## Change description

Before modification: Only one interface can be monitored.

After modification: Multiple interfaces can be monitored. The interfaces in an interface range must be the same type. The start interface number must be smaller than the end interface number.

## Modified feature: Configuring an EAA monitor policy by using Tcl

### Feature change description

In this release, the system uses the platformtools module rather than the Comware module to create a Tcl script file.

### Command changes

N/A

## Modified feature: Displaying the operating status and information of an interface

### Feature change description

In this version and later, the current system time and the last time when the physical state of an interface changed to up or down are displayed in the operating status and information of the interface.

### Command changes

#### Modified command: display interface

##### Syntax

```
display interface [ interface-type [ interface-number | interface-number.subnumber ] ] [ brief [ description | down ] ]
```

##### Views

Any view

#### Command output after modification

```
# Display the operating status and information of Ten-GigabitEthernet 1/0/1.
<Sysname> display interface ten-gigabitethernet 1/0/1
Ten-GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: Ten-GigabitEthernet 1/0/1 Interface
Bandwidth: 10000000 kbps
Maximum transmission unit: 1500
Allow jumbo frames to pass
```

```

Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
Media type is twisted pair
Port priority: 2
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The maximum frame length is 9416
Last link flapping: 6 hours 39 minutes 28 seconds
Last clearing of counters: Never
Current system time:2019-02-10 14:56:12
Last time when physical state changed to up:-
Last time when physical state changed to down:2019-02-10 14:55:25

```

### Change description

Before modification: The current system time and the last time when the physical state of an interface changed to up or down are not displayed in the operating status and information of the interface.

After modification: The current system time and the last time when the physical state of an interface changed to up or down are displayed in the operating status and information of the interface.

## Modified feature: Displaying PFC information of all interfaces

### Feature change description

In this version and later, the PFC information displayed for all interfaces is modified.

### Command changes

#### Modified command: display priority-flow-control interface

##### Syntax

```

display    priority-flow-control    interface    [    interface-type
[ interface-number ] ]

```

##### Views

Any view

### Change description

Before modification:

# Display PFC information of all interfaces.

```
<Sysname> display priority-flow-control interface
```

```
<Sysname> display priority-flow-control interface
```

Interface	AdminMode	OperMode	Dot1pList	Prio	Recv	Send

```
-----
XGE1/0/1          Auto          Disabled  0,2-3,5-6    0      178      43
```

After modification:

# Display PFC information of all interfaces.

```
<Sysname> display priority-flow-control interface
```

```
Conf -- Configured mode   Ne -- Negotiated mode   P -- Priority
```

```
Interface      Conf Ne  Dot1pList   P Recv      Sent
```

```
XGE1/0/1      Auto On   0,2-3,5-6   0 178       43
```

## Modified feature: Link state change suppression on an interface

### Feature change description

In this version, the syntax for configuring link state change suppression on an Ethernet interface is modified. When the link state change suppression interval is configured in seconds on an Ethernet interface, the value range is modified.

### Command changes

#### Modified command: link-delay

##### Old syntax

```
link-delay [ msec ] delay-time [ mode { up | updown } ]
```

```
undo link-delay [ msec ] delay-time [ mode { up | updown } ]
```

##### New syntax

```
link-delay { down | up } [ msec ] delay-time
```

```
undo link-delay { down | up }
```

##### Views

Ethernet interface view

#### Change description

Before modification:

- If the **mode** keyword is not specified, the link-down events are suppressed.
- If the **mode up** keyword combination is specified, the link-up events are suppressed.
- If the **mode updown** keyword combination is specified, both link-down and link-up events are suppressed.
- If the suppression interval configured in the command without the **mode** keyword specified is the same as the suppression interval configured in the command with the **mode up** keyword combination specified on an interface, the two commands are automatically merged into the command with the **mode updown** keyword combination specified in the configuration file of the interface.
- If the **msec** keyword is not specified, the link state change suppression interval is configured in seconds, and the value range is 0 to 30.

After modification:

- If the **down** keyword is not specified, the link-down events are suppressed.
- If the **up** keyword is specified, the link-up events are suppressed.
- You can set different link state change suppression intervals for link-down events and link-up events.
- If the **msec** keyword is not specified, the link state change suppression interval is configured in seconds, and the value range is 0 to 300.

## Modified feature: MAC-to-VLAN entries

### Feature change description

In this version and later, the keyword for configuring 802.1p priorities in MAC-to-VLAN entries is modified to **dot1p**.

### Command changes

#### Modified command: mac-vlan mac-address

##### Old syntax

```
mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ dot1q
priority ]
```

##### New syntax

```
mac-vlan mac-address mac-address [ mask mac-mask ] vlan vlan-id [ dot1p
priority ]
```

##### Views

System view

##### Change description

Before modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is **dot1q**.

After modification: The keyword for configuring 802.1p priorities in MAC-to-VLAN entries is **dot1p**.

#### Modified command: display mac-vlan

##### Syntax

```
display mac-vlan { all | dynamic | mac-address mac-address [ mask mac-mask ]
| static | vlan vlan-id }
```

##### Views

Any view

##### Old command output

# Display all MAC-to-VLAN entries.

```
<Sysname> display mac-vlan all
```

The following MAC VLAN entries exist:

State: S - Static, D - Dynamic

MAC address	Mask	VLAN ID	Dot1q	State
-------------	------	---------	-------	-------

0008-0001-0000	ffff-ff00-0000	5	3	S
0002-0001-0000	ffff-ffff-ffff	5	3	S&D

Total MAC VLAN entries count: 2

## New command output

# Display all MAC-to-VLAN entries.

<Sysname> display mac-vlan all

The following MAC VLAN entries exist:

State: S - Static, D - Dynamic

MAC address	Mask	VLAN ID	Dot1p	State
0008-0001-0000	ffff-ff00-0000	5	3	S
0002-0001-0000	ffff-ffff-ffff	5	3	S&D

Total MAC VLAN entries count: 2

## Change description

Before modification: The field for displaying the 802.1p priority of a VLAN was Dot1q.

After modification: The field for displaying the 802.1p priority of a VLAN was Dot1p.

# Modified feature: Collision handling process of LACP MAD and BFD MAD

## Feature change description

Before modification, LACP MAD and BFD MAD use the following process to handle a multi-active collision:

1. Compare the number of members in each fabric.
2. Set all fabrics to the Recovery state except the one that has the most members.
3. Compare the member IDs of the masters if all IRF fabrics have the same number of members.
4. Set all fabrics to the Recovery state except the one that has the lowest numbered master.

After modification, LACP MAD and BFD MAD use the following process to handle a multi-active collision:

5. Compare the health states (chip forwarding performance states) of split fabrics.
6. Set all fabrics to the Recovery state except the healthiest one.
7. Compare the number of members in each fabric if all IRF fabrics are in the same health state.
8. Set all fabrics to the Recovery state except the one that has the most members.
9. Compare the member IDs of their masters if all IRF fabrics have the same number of members.
10. Set all fabrics to the Recovery state except the one that has the lowest numbered master.

## Command changes

None.

# Modified feature: Collision handling process of ND MAD

## Feature change description

Before modification:

- ND MAD uses the following process to handle a multi-active collision:
  - a. Compares the member IDs of the masters in the IRF fabrics.
  - b. Sets all fabrics to the Recovery state except the one that has the lowest numbered master.
- ND MAD cannot be configured together with ARP MAD because they handle collisions differently.

After modification:

- ND MAD uses the following process to handle a multi-active collision:
  - c. Compares the health states (chip forwarding performance states) of split fabrics.
  - d. Sets all fabrics to the Recovery state except the healthiest one.
  - e. Compares the member IDs of the masters if all IRF fabrics are in the same health state.
  - f. Sets all fabrics to the Recovery state except the one that has the lowest numbered master.
- ND MAD can be configured together with ARP MAD because they use the same collision handling process.

## Command changes

None.

# Modified feature: Displaying global link aggregation load sharing modes

## Feature change description

The default global load sharing modes were modified in the output from the `display link-aggregation load-sharing mode` command.

## Command changes

Modified command: `display link-aggregation load-sharing mode`

### Syntax

```
display link-aggregation load-sharing mode [ interface  
[ { bridge-aggregation | route-aggregation } interface-number ] ]
```

### Views

Any view

### Change description

Before modification: If the default global load sharing modes are used, only **Default** is displayed.

# Display the global link aggregation load sharing modes. This example displays the default settings.

```
<Sysname> display link-aggregation load-sharing mode
```

Link-Aggregation Load-Sharing Algorithm:

Default

Link-Aggregation Load-Sharing Seed:

Default

Link-aggregation load-sharing mode:

Layer 2 traffic: packet type-based sharing

Layer 3 traffic: packet type-based sharing

After modification: If the default global load sharing modes are used, the default values are displayed.

# Display the global link aggregation load sharing modes. This example displays the default settings.

```
<Sysname> display link-aggregation load-sharing mode
```

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

## Modified feature: Configuring a link aggregation load sharing hash seed

### Feature change description

The value range for the load sharing hash seed was changed to 1 to FFFFFFFF.

### Command changes

#### Modified command: link-aggregation global load-sharing seed

##### Syntax

```
link-aggregation global load-sharing seed seed-number
```

##### Views

Any view

##### Change description

Before modification: The value range for the *seed-number* argument is 0 to FFFFFFFF.

After modification: The value range for the *seed-number* argument is 1 to FFFFFFFF.

# Modified feature: Displaying detailed information about the IPP and DR interfaces of DRNI

## Feature change description

The interface numbers of aggregation member ports were added for the local IPP and DR interfaces in the output from the **display drni verbose** command.

## Command changes

### Modified command: display drni verbose

#### Syntax

```
display drni verbose [ interface interface-type interface-number ]
```

#### Views

Any view

#### Change description

Before modification:

# Display detailed information about DR interface Bridge-Aggregation 1.

```
<Sysname> display drni verbose bridge-aggregation 1
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired
```

```
DR interface/DR group ID: BAGG1/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 16385, 16386
Peer Selected ports Index: 32769, 32770
```

# Display detailed information about IPP Bridge-Aggregation 2.

```
<Sysname> display drni verbose bridge-aggregation 2
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
       G -- Port_Sync, H -- Expired
```

```
IPP/IPP ID: BAGG2/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports Index: 16385, 16386
Peer Selected ports Index: 32769, 32770
```

After modification:

# Display detailed information about DR interface Bridge-Aggregation 1.

```
<Sysname> display drni verbose interface bridge-aggregation 1
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
       D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
```



```

G -- Port_Sync, H -- Expired

DR interface/DR group ID: BAGG1/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports (index): XGE1/0/1 (16385), XGE1/0/2 (16386)
Peer Selected ports indexes: 32769, 32770

# Display detailed information about IPP Bridge-Aggregation 2.
<Sysname> display drni verbose interface bridge-aggregation 2
Flags: A -- Home_Gateway, B -- Neighbor_Gateway, C -- Other_Gateway,
      D -- IPP_Activity, E -- DRCP_Timeout, F -- Gateway_Sync,
      G -- Port_Sync, H -- Expired

IPP/IPP ID: BAGG2/1
State: UP
Local state/Peer state: ABDFG/ABDFG
Local Selected ports (index): XGE1/0/1 (16385), XGE1/0/2 (16386)
Peer Selected ports indexes: 32769, 32770

```

## Modified feature: Configuring the advertisable TLVs for LLDP

### Feature change description

From this release, link aggregation TLVs in the IEEE 802.3 organizationally specific TLV set and DCBX TLVs are supported.

[Table 16](#) shows the IEEE 802.3 organizationally specific TLVs.

The Power Stateful Control TLV is defined in IEEE P802.3at D1.0 and is not supported in later versions. The device sends this type of TLVs only after receiving them.

**Table 16 IEEE 802.3 organizationally specific TLVs**

Type	Description
MAC/PHY Configuration/Status	Contains the bit-rate and duplex capabilities of the port, support for autonegotiation, enabling status of autonegotiation, and the current rate and duplex mode.
Link Aggregation	Indicates whether the port supports link aggregation, and if yes, whether link aggregation is enabled.
Power Via MDI	Contains the power supply capabilities of the port: <ul style="list-style-type: none"> <li>• Port class (PSE or PD).</li> <li>• Power supply mode.</li> <li>• Whether PSE power supply is supported.</li> <li>• Whether PSE power supply is enabled.</li> <li>• Whether pair selection can be controlled.</li> <li>• Power supply type.</li> <li>• Power source.</li> <li>• Power priority.</li> <li>• PD requested power.</li> </ul>

Type	Description
	<ul style="list-style-type: none"> <li>PSE allocated power.</li> </ul>
Maximum Frame Size	Indicates the supported maximum frame size.
Power Stateful Control	<p>Indicates the power state control configured on the sending port, including the following:</p> <ul style="list-style-type: none"> <li>Power supply mode of the PSE/PD.</li> <li>PSE/PD priority.</li> <li>PSE/PD power.</li> </ul>
Energy-Efficient Ethernet	Indicates Energy Efficient Ethernet (EEE).

## 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 | congestion-notification |
port-vlan-id | link-aggregation | dcbx | protocol-vlan-id [ vlan-id ] |
vlan-name [ vlan-id ] | management-vid [ mvlan-id ] } | dot3-tlv { all |
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 | congestion-notification |
port-vlan-id | link-aggregation | dcbx | protocol-vlan-id | vlan-name |
management-vid } | dot3-tlv { all | 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 | congestion-notification | port-vlan-id | 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 } }

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 } }

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 } }

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 | 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 } }

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 |
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 } }
```

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 |
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 } }

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 | 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 } }
```

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 } | 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 } | 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 } | 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 }
```

## Change description

The `link-aggregation` and `dcbbx` keywords were added.

# Modified feature: Setting the aging timer for dynamic ARP entries

## Feature change description

In this version and later, you can set the aging timer for dynamic ARP entries in the following views:

- Layer 3 Ethernet interface/subinterface view
- Layer 3 aggregate interface/subinterface view
- VSI interface view
- VLAN interface view

## Command changes

### Modified command: arp timer aging

#### Syntax

```
arp timer aging { aging-minutes | second aging-seconds }
undo arp timer aging
```

#### Views

System view

Layer 3 Ethernet interface/subinterface view

Layer 3 aggregate interface/subinterface view

VSI interface view

VLAN interface view

### Change description

Before modification: This command is supported only in system view.

After modification: This command is supported in system view and the following interface view:

- Layer 3 Ethernet interface/subinterface view
- Layer 3 aggregate interface/subinterface view
- VSI interface view
- VLAN interface view

## Modified feature: ARP snooping

### Feature change description

In this version and later, support for enabling ARP snooping for a VXLAN was added. If you enable ARP snooping for a VXLAN, ARP packets received in the VXLAN are redirected to the CPU. For the VXLAN, the CPU uses the sender IP and MAC addresses of the ARP packets, VSI name, and link ID to create ARP snooping entries.

### Command changes

#### Modified command: arp snooping enable

##### Syntax

```
arp snooping enable
```

##### Views

VLAN view

VSI view

##### Change description

Before modification: This command is supported only in VLAN view.

After modification: This command is supported in both VLAN view and VSI view.

#### Modified command: display arp snooping

##### Old syntax

```
display arp snooping [ vlan vlan-id ] [ slot slot-number ] [ count ]
```

```
display arp snooping ip ip-address [ slot slot-number ]
```

##### New syntax

```
display arp snooping { vlan [ vlan-id ] | vsi [ vsi-name ] } [ slot slot-number ]  
[ count ]
```

```
display arp snooping vlan ip ip-address [ slot slot-number ]
```



## Views

Any view

## Change description

Before modification: Displaying ARP snooping entries for a VSI is not supported.

After modification: Displaying ARP snooping entries for a VSI is supported.

## Modified command: reset arp snooping

### Old syntax

```
reset arp snooping [ ip ip-address | vlan vlan-id ]
```

### New syntax

```
reset arp snooping { vlan [ vlan-id ] | vsi [ vsi-name ] }  
reset arp snooping vlan ip ip-address
```

## Views

Any view

## Change description

Before modification: You can clear ARP snooping entries only for a VLAN, ARP snooping entries for the specified IP address in VLANs, or all ARP snooping entries. The syntax for the command to clear ARP snooping entries for the specified IP address in VLANs is **reset arp snooping ip *ip-address***.

After modification: You can also clear ARP snooping entries for a VSI, for all VSIs, or for all VLANs. The syntax for the command to clear ARP snooping entries for the specified IP address in VLANs is **reset arp snooping vlan ip *ip-address***.

# Modified feature: Specifying DHCP servers for a DHCP relay address pool

## Feature change description

This release supports specifying DHCP servers in VPN instances for a DHCP relay address pool.

## Command changes

### Modified command: remote-server

#### Old syntax

```
remote-server ip-address&<1-8>
```

#### New syntax

```
remote-server ip-address&<1-8> [ public | vpn-instance  
vpn-instance-name ]  
undo remote-server [ ip-address&<1-8> ]
```

## Views

DHCP address pool view

## Change description

Before modification: The command supports only specifying DHCP servers on the public network for a DHCP relay address pool.

After modification: The command supports specifying DHCP servers on the public network and VPN instances for a DHCP relay address pool.

# Modified feature: Displaying DHCP snooping and DHCPv6 snooping trusted ports

## Feature change description

This release added support for displaying DHCP snooping and DHCPv6 snooping trusted ports in VSIs.

## Command changes

### Modified command: display dhcp snooping trust

#### Syntax

```
display dhcp snooping trust
```

#### Views

Any view

## Change description

Before modification: This command displays trusted ports only in VLANs.

# Display information about trusted ports.

```
<Sysname> display dhcp snooping trust
```

```
DHCP snooping is enabled.
```

Interface	Trusted	VLAN
=====	=====	=====
Ten-GigabitEthernet1/0/1	Trusted	
Ten-GigabitEthernet1/0/2	-	100
Ten-GigabitEthernet1/0/3	-	100, 200

**Table 1 Command output**

Field	Description
Interface	Interface name.
Trusted	For a DHCP snooping trusted port specified in the global DHCP snooping configuration, this field displays <b>Trusted</b> . For a trusted port specified in VLAN-based DHCP snooping configuration, this field displays a hyphen (-).
VLAN	VLAN to which the trusted port belongs. If the trusted port is specified in global DHCP snooping configuration, the field value is empty.

After modification: This command supports displaying trusted ports in VLANs and VSIs.

# Display information about trusted ports.

```

<Sysname> display dhcp snooping trust
  DHCP snooping is enabled.
Interface                                     Trusted  VLAN
=====
XGE1/0/1                                     Trusted  -
XGE1/0/2                                     -        100
VSI name                                     Tunnel trusted
=====
a                                              Trusted
AC                                              Trusted
=====
XGE1/0/1 srv 1                               Trusted

```

**Table 2 Command output**

Field	Description
Interface	Interface name.
Trusted	For a DHCP snooping trusted port specified in the global DHCP snooping configuration, this field displays <b>Trusted</b> . For a trusted port specified in VLAN-based DHCP snooping configuration, this field displays a hyphen (-).
VLAN	VLAN to which the trusted port belongs. If the trusted port is specified in global DHCP snooping configuration, this field displays a hyphen (-).
VSI name	VSI name of the VXLAN tunnel interface. This field is available when you configure the tunnel interface assigned to the VSI as a DHCP snooping trusted interface by using the <b>dhcp snooping trust tunnel</b> command.
Tunnel trusted	Trusted tunnel interface specified in VXLAN-based DHCP snooping configuration.
AC	AC name, which is indicated by the interface name and Ethernet service instance name. This field is available when you configure the AC as the DHCP snooping trusted interface by using the <b>dhcp snooping trust</b> command in Ethernet service instance view.
Trusted	Trusted AC specified in VXLAN-based DHCP snooping configuration.

Modified command: display ipv6 dhcp snooping trust

## Syntax

```
display ipv6 dhcp snooping trust
```

## Views

Any view

## Change description

Before modification: This command displays information about trusted ports only in VLANs.

# Display information about trusted ports.

```

<Sysname> display ipv6 dhcp snooping trust
DHCPv6 snooping is enabled.

```

```

Interface                                     Trusted
=====                                     =====
Ten-GigabitEthernet1/0/1                     Trusted

VSI(Trust tunnel)                             Trusted
=====                                     =====

Interface          SrvID                     Trusted
=====          =====          =====
XGE1/0/1           1                       Trusted

```

**Table 3 Command output**

Field	Description
Interface	Interface name.
VSI(Trust tunnel)	This field is not supported in the current software version. VSI name. This field is available when you configure the VXLAN tunnel interfaces assigned to the VSI as a DHCP snooping trusted interface by using the <b>ipv6 dhcp snooping trust tunnel</b> command.
SrvID	This field is not supported in the current software version. ID of the Ethernet service instance on which the mapped AC is configured as a DHCP snooping trusted interface.
Trusted	DHCP snooping trusted interface. This field displays <b>Trusted</b> if the interface is configured as trusted after the DHCPv6 snooping is enabled.

After modification: This command supports displaying trusted ports in VLANs and VSIs.

#### # Display information about trusted ports.

```
<Sysname> display ipv6 dhcp snooping trust
```

DHCPv6 snooping is enabled.

```

Interface                                     Trusted      VLAN
=====                                     =====      =====
XGE1/0/1                                     -            100
XGE1/0/2                                     Trusted      -

```

```

VSI name                                     Tunnel trusted
=====                                     =====
a                                             Trusted

```

```

AC                                             Trusted
=====                                     =====
XGE1/0/1 srv 1                               Trusted

```

**Table 17 Command output**

Field	Description
Interface	Interface name.
Trusted	Trusted port specified in global DHCPv6 snooping configuration. If the trusted port is specified in VLAN-based DHCPv6 snooping configuration, this field displays a hyphen (-).

Field	Description
VLAN	VLAN to which the trusted port belongs. If the trusted port is specified in global DHCPv6 snooping configuration, this field displays a hyphen (-).
VSI name	VSI name of the VXLAN tunnel interface. This field is available when you configure the tunnel interface assigned to the VSI as a DHCP snooping trusted interface by using the <b>ipv6 dhcp snooping trust tunnel</b> command.
Tunnel trusted	Trusted tunnel interface specified in VXLAN-based DHCPv6 snooping configuration.
AC	AC name, which is indicated by the interface name and Ethernet service instance name. This field is available when you configure the AC as the DHCPv6 snooping trusted interface by using the <b>ipv6 dhcp snooping trust</b> command in Ethernet service instance view.
Trusted	Trusted AC specified in VXLAN-based DHCPv6 snooping configuration.

## Modified feature: Displaying DHCP address pool information

### Feature change description

The **display dhcp server pool** command output supports displaying the time unit for the lease duration.

### Command changes

#### Modified command: display dhcp server pool

##### Syntax

```
display dhcp server pool [ pool-name | vpn-instance vpn-instance-name ]
```

##### Views

Any view

##### Change description

The time unit was added to the lease duration in the command output.

# Display information about all DHCP pools.

```
<Sysname> display dhcp server pool
```

```
Pool name: 0
```

```
Network 20.1.1.0 mask 255.255.255.0
```

```
class a range 20.1.1.50 20.1.1.60
```

```
bootfile-name abc.cfg
```

```
dns-list 20.1.1.66 20.1.1.67 20.1.1.68
```

```
domain-name www.aabbcc.com
```

```
bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQP1791YvQoF2Gs1E+65LOU=
```

```
option 2 ip-address 1.1.1.1
```

```
expired day 1 hour 2 minute 3 second 0
```

```

Pool name: 1
Network 20.1.2.0 mask 255.255.255.0
secondary networks:
    20.1.3.0 mask 255.255.255.0
    20.1.4.0 mask 255.255.255.0
bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQP791YvQoF2Gs1E+65LOU=
forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
gateway-list 20.1.1.1 20.1.1.2 20.1.1.4
nbns-list 20.1.1.5 20.1.1.6 20.1.1.7
netbios-type m-node
option 2 ip-address 1.1.1.1
expired day 1 hour 0 minute 0 second 0

```

```

Pool name: 2
Network 20.1.3.0 mask 255.255.255.0
address range 20.1.3.1 to 20.1.3.15
class departmentA range 20.1.3.20 to 20.1.3.29
class departmentB range 20.1.3.30 to 20.1.3.40
next-server 20.1.3.33
tftp-server domain-name www.dian.org.cn
tftp-server ip-address 192.168.0.120
voice-config ncp-ip 20.1.3.2
voice-config as-ip 20.1.3.5
voice-config voice-vlan 3 enable
voice-config fail-over 20.1.3.6 123*
option 2 ip-address 20.1.3.10
expired day 1 hour 0 minute 0 second 0

```

```

Pool name: 3
static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
        hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
        client-identifier aaaa-bbbb
expired unlimited

```

**Table 18 Command output**

Field	Description
Pool name	Name of an address pool. If the address pool is assigned by the OVSDB controller, the pool name starts with a question mark (?). For more information about OVSDB, see OVSDB VTEP configuration in <i>VXLAN Configuration Guide</i> .
Network	Assignable network.
secondary networks	Assignable secondary networks.
address range	Assignable address range.
class <i>class-name</i> range	DHCP user class and its address range.

static bindings	Static IP-to-MAC/client ID bindings.
option	Customized DHCP option.
expired	Lease duration.
bootfile-name	Boot file name
dns-list	DNS server IP address.
domain-name	Domain name suffix.
bims-server	BIMS server information.
forbidden-ip	IP addresses excluded from dynamic allocation.
gateway-list	Gateway addresses.
nbns-list	WINS server addresses.
netbios-type	NetBIOS node type.
next-server	Next server IP address.
tftp-server domain-name	TFTP server name.
tftp-server ip-address	TFTP server address.
voice-config ncp-ip	Primary network calling processor address.
voice-config as-ip	Backup network calling processor address.
voice-config voice-vlan	Voice VLAN.
voice-config fail-over	Failover route.

## Modified feature: Displaying DHCPv6 address pool information

### Feature change description

The **display ipv6 dhcp pool** command output supports displaying the time unit for the preferred lifetime and valid lifetime.

### Command changes

#### Modified command: display ipv6 dhcp pool

##### Syntax

```
display ipv6 dhcp pool [ pool-name | vpn-instance vpn-instance-name ]
```

##### Views

Any view

##### Examples

After modification, the time unit is added to the preferred lifetime and valid lifetime.

The following shows the examples.

# Display information about DHCPv6 address pool 1.

```
<Sysname> display ipv6 dhcp pool 1
```

```

DHCPv6 pool: 1
  Network: 3FFE:501:FFFF:100::/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  Prefix pool: 1
    Preferred lifetime 24000 seconds, valid lifetime 36000 seconds
  Addresses:
    Range: from 3FFE:501:FFFF:100::1
          to 3FFE:501:FFFF:100::99
    Preferred lifetime 70480 seconds, valid lifetime 200000 seconds
    Total address number: 153
    Available: 153
    In-use: 0
  Temporary addresses:
    Range: from 3FFE:501:FFFF:100::200
          to 3FFE:501:FFFF:100::210
    Preferred lifetime 60480 seconds, valid lifetime 259200 seconds
    Total address number: 17
    Available: 17
    In-use: 0
  Static bindings:
    DUID: 0003000100e0fc0000001
    IAID: 0000003f
    Prefix: 3FFE:501:FFFF:200::/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
    DUID: 0003000100e0fc00c0ff1
    IAID: 00000001
    Address: 3FFE:501:FFFF:2001::1/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  DNS server addresses:
    2::2
  Domain name:
    aaa.com
  SIP server addresses:
    5::1
  SIP server domain names:
    bbb.com

```

**# Display information about DHCPv6 address pool 1, which contains an ineffective subnet prefix.**

```
<Sysname> display ipv6 dhcp pool 1
```

```

DHCPv6 pool: 1
  Network: Not-available
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

```

**# Display information about DHCPv6 address pool 1, in which the subnet prefix is ineffective after a configuration recovery.**

```
<Sysname> display ipv6 dhcp pool 1
```

```

DHCPv6 pool: 1
  Network: 1::/64(Zombie)
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

```



**Table 19 Command output**

Field	Description
DHCPv6 pool	Name of the DHCPv6 address pool.
Network	IPv6 subnet for dynamic IPv6 address allocation. If the subnet prefix is ineffective, this field displays <b>Not-available</b> . If the subnet prefix becomes ineffective after a configuration recovery (for example, a switchover from the backup to the master), the prefix is marked ( <b>Zombie</b> ).
Prefix pool	Prefix pool referenced by the address pool.
Preferred lifetime	Preferred lifetime in seconds.
valid lifetime	Valid lifetime in seconds.
Addresses	Non-temporary IPv6 address range.
Range	IPv6 address range for dynamic allocation.
Total address number	Total number of IPv6 addresses.
Available	Total number of available IPv6 addresses.
In-use	Total number of assigned IPv6 addresses.
Temporary addresses	Temporary IPv6 address range for dynamic allocation.
Static bindings	Static bindings configured in the address pool.
DUID	Client DUID.
IAID	Client IAID. If no IAID is configured, this field displays <b>Not configured</b> .
Prefix	IPv6 address prefix.
Address	Static IPv6 address.
DNS server addresses	DNS server address.
Domain name	Domain name.
SIP server addresses	SIP server address.
SIP server domain names	Domain name of the SIP server.

## Modified feature: Enabling recording DHCPv6 snooping address entries in VLAN view

### Feature change description

This release added support of enabling recording DHCPv6 snooping address entries in VLAN view.

## Command changes

Modified command: ipv6 dhcp snooping binding record

### Syntax

```
ipv6 dhcp snooping binding record
undo ipv6 dhcp snooping binding record
```

### Change description

Before modification: This command is available in Layer 2 Ethernet interface view and Layer 2 aggregate interface view.

After modification: This command is available in Layer 2 Ethernet interface view, Layer 2 aggregate interface view, and VLAN view.

## Modified feature: Setting the aging timer for ND entries in stale state

### Feature change description

This release supports setting the aging timer in seconds for ND entries in stale state.

## Command changes

### Old syntax

```
ipv6 neighbor stale-aging aging-time
```

### New syntax

```
ipv6 neighbor stale-aging { aging-minutes | second aging-seconds }
```

### Parameters

*aging-minutes*: Specifies the aging timer in minutes for ND entries in stale state, in the range of 1 to 1440.

**second** *aging-seconds*: Specifies the aging timer in seconds for ND entries in stale state, in the range of 60 to 86400.

### Change description

Before modification: The aging timer can be set in minutes for ND entries in stale state.

After modification: The aging timer can be set in minutes or in seconds for ND entries in stale state.

## Modified feature: Displaying member interfaces shut down by Monitor Link

### Feature change description

From this release, the **display monitor-link group** command displays the member interfaces shut down by Monitor Link.

## Command changes

Modified command: display monitor-link group

### Syntax

```
display monitor-link group { group-id | all }
```

### Views

Any view

### Change description

Before modification: The **display monitor-link group** command does not display the member interfaces shut down by Monitor Link.

After modification: The **display monitor-link group** command displays the member interfaces shut down by Monitor Link.

## Modified feature: Displaying DLDP configuration

### Feature change description

The following fields were added to the command output:

- DLDP initial-unidirectional-delay.
- Neighbor echo time.

## Command changes

Modified command: display dldp

### Syntax

```
display dldp [ interface interface-type interface-number ]
```

### Views

Any view

### Change description

After modification, the command displays the **DLDP initial-unidirectional-delay** and **Neighbor echo time** fields.

```
<Sysname> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: Simple
DLDP authentication-password: *****
DLDP unidirectional-shutdown mode: Auto
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface Ten-GigabitEthernet1/0/1
DLDP port state: Bidirectional
DLDP port unidirectional-shutdown mode: None
```

DLDP initial-unidirectional-delay: 100s

Number of the port's neighbors: 1

Neighbor MAC address: 0023-8956-3600

Neighbor port index: 79

Neighbor state: Confirmed

Neighbor aged time: 13s

Neighbor echo time: -

**Table 4 Command output**

Field	Description
DLDP initial-unidirectional-delay	Delay time in seconds for DLDP to block the interface upon an Initial-to-Unidirectional state transition.
Neighbor echo time	Number of seconds remaining before the Echo timer expires. The Echo timer starts when the Entry timer expires. The neighbor information is deleted when the Echo timer expires. A hyphen (-) indicates that the Echo timer has not started.

## Modified feature: Configuring routing policy-based recursive lookup

### Feature change description

Support for IPv6 BGP routes in RIB IPv6 address family view was added to this release.

### Command changes

#### Modified command: protocol nexthop recursive-lookup

##### Syntax

```
protocol protocol nexthop recursive-lookup route-policy  
route-policy-name
```

```
undo protocol protocol nexthop recursive-lookup route-policy
```

##### Views

RIB IPv4 address family view

RIB IPv6 address family view

##### Change description

Before modification: The command supports only BGP and static routes in RIB IPv4 address family view.

After modification: The command also supports IPv6 BGP routes in RIB IPv6 address family view.

# Modified feature: Associating Track with the output interface for a static route

## Feature change description

In this release, you can associate a track entry with the output interface for a static route.

## Command changes

### Modified command: ip route-static

#### Old syntax

```
ip route-static { dest-address { mask-length | mask } | group group-name }  
{ interface-type interface-number [ next-hop-address ] [ backup-interface  
interface-type interface-number [ backup-nexthop backup-nexthop-address ]  
[ permanent ] | bfd { control-packet | echo-packet } | permanent ] |  
next-hop-address [ recursive-lookup host-route ] [ bfd control-packet  
bfd-source ip-address | permanent | track track-entry-number ] |  
vpn-instance d-vpn-instance-name next-hop-address [ recursive-lookup  
host-route ] [ bfd control-packet bfd-source ip-address | permanent | track  
track-entry-number ] } [ preference preference ] [ tag tag-value ]  
[ description text ]
```

```
ip route-static vpn-instance s-vpn-instance-name { dest-address  
{ mask-length | mask } | group group-name } { interface-type  
interface-number [ next-hop-address ] [ backup-interface interface-type  
interface-number [ backup-nexthop backup-nexthop-address ] [ permanent ] |  
bfd { control-packet | echo-packet } | permanent ] | next-hop-address  
[ recursive-lookup host-route ] [ public ] [ bfd control-packet bfd-source  
ip-address | permanent | track track-entry-number ] | vpn-instance  
d-vpn-instance-name next-hop-address [ recursive-lookup host-route ]  
[ bfd control-packet bfd-source ip-address | permanent | track  
track-entry-number ] } [ preference preference ] [ tag tag-value ]  
[ description text ]
```

#### New syntax

```
ip route-static { dest-address { mask-length | mask } | group group-name }  
{ interface-type interface-number [ next-hop-address ] [ backup-interface  
interface-type interface-number [ backup-nexthop backup-nexthop-address ]  
[ permanent ] | bfd { control-packet | echo-packet } | permanent | track  
track-entry-number ] | next-hop-address [ recursive-lookup host-route ]  
[ bfd control-packet bfd-source ip-address | permanent | track  
track-entry-number ] | vpn-instance d-vpn-instance-name next-hop-address  
[ recursive-lookup host-route ] [ bfd control-packet bfd-source ip-address  
| permanent | track track-entry-number ] } [ preference preference ] [ tag  
tag-value ] [ description text ]
```

```
ip route-static vpn-instance s-vpn-instance-name { dest-address  
{ mask-length | mask } | group group-name } { interface-type  
interface-number [ next-hop-address ] [ backup-interface interface-type  
interface-number [ backup-nexthop backup-nexthop-address ] [ permanent ] |  
bfd { control-packet | echo-packet } | permanent | track track-entry-number ]  
| next-hop-address [ recursive-lookup host-route ] [ public ] [ bfd  
control-packet bfd-source ip-address | permanent | track
```

```
track-entry-number ] | vpn-instance d-vpn-instance-name next-hop-address
[ recursive-lookup host-route ] [ bfd control-packet bfd-source ip-address
| permanent | track track-entry-number ] } [ preference preference ] [ tag
tag-value ] [ description text ]
```

## Views

System view

## Change description

Before modification: You cannot associate a track entry with the output interface for a static route.

After modification: You can associate a track entry with the output interface for a static route.

# Modified feature: Configuring OSPF area authentication

## Feature change description

From this release, a key ID becomes optional in HMAC-MD5 and MD5 authentication modes, and a key string becomes optional in simple authentication mode.

## Command changes

### Modified command: authentication-mode

#### Old syntax

In MD5/HMAC-MD5 authentication mode:

```
authentication-mode { hmac-md5 | md5 } key-id { cipher | plain } string
undo authentication-mode [ { hmac-md5 | md5 } key-id ]
```

In simple authentication mode:

```
authentication-mode simple { cipher | plain } string
undo authentication-mode
```

#### New syntax

In MD5/HMAC-MD5 authentication mode:

```
authentication-mode { hmac-md5 | md5 } [ key-id { cipher | plain } string ]
undo authentication-mode [ { hmac-md5 | md5 } [ key-id ] ]
```

In simple authentication mode:

```
authentication-mode simple [ { cipher | plain } string ]
undo authentication-mode
```

## Views

OSPF area view

## Change description

Before modification: A key ID is required in HMAC-MD5 and MD5 authentication modes, and a key string is required in simple authentication mode.

After modification: A key ID is optional in HMAC-MD5 and MD5 authentication modes, and a key string is optional in simple authentication mode.

# Modified feature: Configuring OSPF interface authentication

## Feature change description

From this release, a key ID becomes optional in HMAC-MD5 and MD5 authentication modes, a key string becomes optional in simple authentication mode, and the none authentication mode is supported.

## Command changes

### Modified command: ospf authentication-mode

#### Old syntax

In MD5/HMAC-MD5 authentication mode:

```
ospf authentication-mode { hmac-md5 | md5 } key-id { cipher | plain } string
undo ospf authentication-mode { hmac-md5 | md5 } key-id
```

In simple authentication mode:

```
ospf authentication-mode simple { cipher | plain } string
undo ospf authentication-mode simple
```

#### New syntax

In MD5/HMAC-MD5 authentication mode:

```
ospf authentication-mode { hmac-md5 | md5 } [ key-id { cipher | plain }
string ]
undo ospf authentication-mode { hmac-md5 | md5 } [ key-id ]
```

In simple authentication mode:

```
ospf authentication-mode simple [ { cipher | plain } string ]
undo ospf authentication-mode simple
```

In none authentication mode:

```
ospf authentication-mode none
undo ospf authentication-mode none
```

#### Views

Interface view

#### Change description

Before modification: A key ID is required in HMAC-MD5 and MD5 authentication modes, a key string is required in simple authentication mode, and the none authentication mode is not supported.

After modification: A key ID is optional in HMAC-MD5 and MD5 authentication modes, a key string is optional in simple authentication mode, and the none authentication mode is supported.

## Modified feature: Configuring a virtual link

### Feature change description

From this release, a key ID becomes optional in HMAC-MD5 and MD5 authentication modes, a key string becomes optional in simple authentication mode, and the none authentication mode is supported.

### Command changes

#### Modified command: vlink-peer

##### Old syntax

```
vlink-peer router-id [ dead seconds | hello seconds | { { 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 | { hmac-md5 | md5 } key-id |  
keychain | retransmit | simple | trans-delay ] *
```

##### New 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 ]  
*
```

### Views

Interface view

### Change description

Before modification: A key ID is required in HMAC-MD5 and MD5 authentication modes, a key string is required in simple authentication mode, and the none authentication mode is not supported.

After modification: A key ID is optional in HMAC-MD5 and MD5 authentication modes, a key string is optional in simple authentication mode, and the none authentication mode is supported.

## Modified feature: Setting the number of OSPF logs

### Feature change description

From this release, you can set the number of logs for the following types of hello packets:

- Received hello packets.
- Received abnormal hello packets.
- Received hello packets that were dropped.
- Sent hello packets.
- Sent abnormal hello packets.
- Hello packets that failed to be sent.



The maximum number of LSA aging, neighbor state change, or route calculation logs that OSPF can generate by default is also changed in this release.

## Command changes

### Modified command: event-log

#### Old syntax

```
event-log { lsa-flush | peer | spf } size count  
undo event-log { lsa-flush | peer | spf } size
```

#### New syntax

```
event-log { hello { received [ abnormal | dropped ] | sent [ abnormal |  
failed ] } | lsa-flush | peer | spf } size count  
undo event-log { hello { received [ abnormal | dropped ] | sent [ abnormal |  
failed ] } | lsa-flush | peer | spf } size
```

#### Views

OSPF view

#### Change description

Before modification:

- The **hello**, **received**, **sent**, **abnormal**, **dropped**, and **failed** keywords are not supported. You cannot set the number of logs for hello packets.
- OSPF can generate a maximum of 10 LSA aging, neighbor state change, or route calculation logs by default.

After modification:

- The **hello**, **received**, **sent**, **abnormal**, **dropped**, and **failed** keywords are added to this command to enable you to set the number of logs for hello packets.
- OSPF can generate a maximum of 100 LSA aging, neighbor state change, or route calculation logs by default.

## Modified feature: Displaying IS-IS LSP log information

### Feature change description

From this release, you must specify the **refreshed** or **purged** keyword when displaying IS-IS LSP log information.

## Command changes

#### Old syntax

```
display isis event-log lsp [ level-1 | level-2 ] [ process-id ]
```

#### New syntax

```
display isis event-log lsp { purged | refreshed } [ level-1 | level-2 ]  
[ process-id ]
```

## Change description

Before modification, the **refreshed** and **purged** keywords are not available.

After modification, you must specify the **refreshed** or **purged** keyword for the command.

# Modified feature: Clearing IS-IS LSP log information

## Feature change description

From this release, you must specify the **refreshed** or **purged** keyword when clearing IS-IS LSP log information.

## Command changes

### Old syntax

```
reset isis event-log lsp [ process-id ]
```

### New syntax

```
reset isis event-log lsp { purged | refreshed } [ process-id ]
```

## Change description

Before modification, the **refreshed** and **purged** keywords are not available.

After modification, you must specify the **refreshed** or **purged** keyword for the command.

# Modified feature: Specifying a label allocation mode

## Feature change description

From this release, BGP supports allocating a label to each VPN instance.

## Command changes

### Modified command: **label-allocation-mode**

#### Old syntax

```
label-allocation-mode per-prefix
```

#### New syntax

```
label-allocation-mode { per-prefix | per-vrf }
```

#### Views

BGP instance view

## Change description

Before modification, BGP does not support allocating a label to each VPN instance.

After modification, BGP supports allocating a label to each VPN instance. When you specify the per-VPN instance label allocation mode, do not execute the **vpn popgo** command because it is mutually exclusive with the **label-allocation-mode per-vrf** command. The egress PE will pop the label for each packet and forward the packet through the FIB table.

# Modified feature: Displaying BGP peer or peer group information

## Feature change description

Support for displaying peer or peer group information of all VPN instances was added to BGP.

## Command changes

Modified command: display bgp peer

### Old syntax

```
display bgp [ instance instance-name ] peer ipv4 [ unicast ] vpn-instance  
vpn-instance-name [ [ ipv4-address ] verbose ]
```

```
display bgp [ instance instance-name ] peer ipv6 [ unicast ] vpn-instance  
vpn-instance-name [ [ ipv6-address ] verbose ]
```

### New syntax

```
display bgp [ instance instance-name ] peer ipv4 [ unicast ] { vpn-instance  
vpn-instance-name [ [ ipv4-address ] verbose ] | vpn-instance-all  
[ verbose ] }
```

```
display bgp [ instance instance-name ] peer ipv6 [ unicast ] { vpn-instance  
vpn-instance-name [ [ ipv6-address ] verbose ] | vpn-instance-all  
[ verbose ] }
```

### Views

BGP instance view

### Change description

Before modification: BGP cannot display peer or peer group information for all VPN instances.

After modification: BGP can display peer or peer group information for all VPN instances.

# Modified feature: Displaying AS path information for BGP routes

## Feature change description

A maximum of 16 AS numbers can be displayed for the Path/Ogn field in the output from the following commands (exceeding AS numbers are omitted and are available by displaying detailed routing information):

- display bgp link-state
- display bgp routing-table dampened
- display bgp routing-table flap-info
- display bgp routing-table ipv4 multicast
- display bgp routing-table ipv4 rtfilter
- display bgp routing-table ipv4 unicast

- `display bgp routing-table ipv6 multicast`
- `display bgp routing-table ipv6 unicast`

## Command changes

### Syntax

```
display bgp [ instance instance-name ] link-state [ ls-prefix | peer
{ ipv4-address | ipv6-address } { advertised | received } [ statistics ] |
statistics ]

display bgp [ instance instance-name ] routing-table dampened { ipv4 |
ipv6 } { multicast | [ unicast ] [ vpn-instance vpn-instance-name ] }

display bgp [ instance instance-name ] routing-table flap-info ipv4
{ multicast | [ unicast ] [ vpn-instance vpn-instance-name ] }
[ ipv4-address [ { mask-length | mask } [ longest-match ] ] | as-path-acl
as-path-acl-number ]

display bgp [ instance instance-name ] routing-table flap-info ipv6
{ multicast | [ unicast ] [ vpn-instance vpn-instance-name ] }
[ ipv6-address prefix-length | as-path-acl as-path-acl-number ]

display bgp [ instance instance-name ] routing-table ipv4 multicast
[ ipv4-address [ { mask-length | mask } [ longest-match ] ] | ipv4-address
[ mask-length | mask ] advertise-info | as-path-acl as-path-acl-number |
community-list { { basic-community-list-number | comm-list-name }
[ whole-match ] | adv-community-list-number } | peer ipv4-address
{ advertised-routes | received-routes } [ ipv4-address [ mask-length | mask ]
| statistics ] | statistics ]

display bgp [ instance instance-name ] routing-table ipv4 [ unicast ]
[ vpn-instance vpn-instance-name ] [ ipv4-address [ { mask-length | mask }
[ longest-match ] ] | ipv4-address [ mask-length | mask ] advertise-info |
as-path-acl as-path-acl-number | community-list
{ { basic-community-list-number | comm-list-name } [ whole-match ] |
adv-community-list-number } | peer ipv4-address { advertised-routes |
received-routes } [ ipv4-address [ mask-length | mask ] | statistics ] |
statistics ]

display bgp [ instance instance-name ] routing-table ipv6 multicast
[ ipv6-address prefix-length [ advertise-info ] | as-path-acl
as-path-acl-number | community-list { { basic-community-list-number |
comm-list-name } [ whole-match ] | adv-community-list-number } | peer
ipv6-address { advertised-routes | received-routes } [ ipv6-address
prefix-length | statistics ] | statistics ]

display bgp [ instance instance-name ] routing-table ipv6 [ unicast ]
[ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length
[ advertise-info ] | as-path-acl as-path-acl-number | community-list
{ { basic-community-list-number | comm-list-name } [ whole-match ] |
adv-community-list-number } | peer ipv6-address { advertised-routes |
received-routes } [ ipv6-address prefix-length | statistics ] |
statistics ]

display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] peer
ipv4-address { advertised-routes | received-routes } [ ipv6-address
prefix-length | statistics ]
```

## Views

Any view

### Change description

Before modification, all AS numbers are displayed for the Path/Ogn field in the command output, as shown in the following example.

# Display brief information about all BGP IPv4 unicast routes.

```
<Sysname> display bgp routing-table ipv4
```

Total number of routes: 4

BGP local router ID is 192.168.100.1

Status codes: \* - valid, > - best, d - dampened, h - history,  
s - suppressed, S - stale, i - internal, e - external  
a - additional-path  
Origin: i - IGP, e - EGP, ? - incomplete

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >	10.2.1.0/24	10.2.1.1	0		0	i
e		10.2.1.2	0		0	200 201
						202 203
						204 205
						206 207
						208 209
						210 211
						212 213
						214 215
						216 217
						218i
* >	192.168.1.0	192.168.1.135	0		0	i
* e		10.2.1.2	0		0	200i

After modification, a maximum of 16 AS numbers can be displayed for the Path/Ogn field in the command output. Exceeding AS numbers are omitted and are available by displaying detailed routing information.

# Display brief information about all BGP IPv4 unicast routes.

```
<Sysname> display bgp routing-table ipv4
```

Total number of routes: 4

BGP local router ID is 192.168.100.1

Status codes: \* - valid, > - best, d - dampened, h - history,  
s - suppressed, S - stale, i - internal, e - external  
a - additional-path  
Origin: i - IGP, e - EGP, ? - incomplete

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
--	---------	---------	-----	--------	---------	----------

```

* > 10.2.1.0/24      10.2.1.1      0      0      i
    e                10.2.1.2      0      0      200 201
202 203 204 205 206 207 208 209 210 211 212 213 214 215 ...i
* > 192.168.1.0      192.168.1.135  0      0      i
* e                10.2.1.2      0      0      200i

```

## Modified feature: Displaying RPF information for an IPv6 multicast source

### Feature change description

Support for displaying the AS number of the source-side PE and the route target attribute of the C-multicast route was added.

### Command changes

#### Modified command: display ipv6 multicast rpf-info

##### Syntax

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] rpf-info
ipv6-source-address [ ipv6-group-address ]
```

##### Views

Any view

##### Change description

Before modification: The **Source AS** and **C-multicast route target** fields are not supported.

# Display RPF information for IPv6 multicast source 2001::101 on the public network.

```

<Sysname> display ipv6 multicast rpf-info 2001::101
RPF information about source 2001::101:
  RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:101:1
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable

```

After modification: The **Source AS** and **C-multicast route target** fields are supported.

# Display RPF information for IPv6 multicast source 2001::101 on the public network.

```

<Sysname> display ipv6 multicast rpf-info 2001::101
RPF information about source 2001::101:
  RPF interface: Vlan-interface1, RPF neighbor: FE80::A01:101:1
  Referenced prefix/prefix length: 2001::/64
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
  Source AS: 0
  C-multicast route target: 0x0000000000000000

```

**Table 20 Command output**

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101.
RPF interface	Type and number of the RPF interface.
RPF neighbor	IPv6 address (link-local address) of the RPF neighbor.
Referenced prefix/prefix length	Referenced route and its prefix length.
Referenced route type	Type of the referenced route: <ul style="list-style-type: none"> <li>• <b>igp</b>—IPv6 IGP unicast route.</li> <li>• <b>egp</b>—IPv6 EGP unicast route.</li> <li>• <b>unicast (direct)</b> —IPv6 directly connected unicast route.</li> <li>• <b>unicast</b>—Other IPv6 unicast route, such as IPv6 unicast static route.</li> <li>• <b>mbgp</b>—IPv6 MBGP route.</li> </ul>
Route selection rule	RPF route selection rule: <ul style="list-style-type: none"> <li>• Route preference.</li> <li>• Longest prefix match.</li> </ul>
Load splitting rule	Whether load splitting is enabled.
Source AS	AS number of the source-side PE. NOTE: This field is supported in this version and later.
C-multicast route target	Route target attribute value of the C-multicast route. NOTE: This field is supported in this version and later.

## Modified feature: Displaying statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping

### Feature change description

The layout of command output was changed and support for displaying the number of IGMP messages received on the DRNI IPP was added.

### Command changes

#### Modified command: display igmp-snooping statistics

##### Syntax

```
display igmp-snooping statistics
```

##### Views

Any view

## Change description

Before modification: The **DRNI** field is not supported.

# Display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries: 0
Received IGMPv1 reports: 0
Received IGMPv2 reports: 19
Received IGMP leaves: 0
Received IGMPv2 specific queries: 0
Sent IGMPv2 specific queries: 0
Received IGMPv3 reports: 1
Received IGMPv3 reports with right and wrong records: 0
Received IGMPv3 specific queries: 0
Received IGMPv3 specific sg queries: 0
Sent IGMPv3 specific queries: 0
Sent IGMPv3 specific sg queries: 0
Received PIMv2 hello: 0
Received error IGMP messages: 19
```

After modification: The **DRNI** field is supported.

# Display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP messages:
  IGMP general queries: 19
  DRNI: 19
  IGMPv2 specific queries: 10
  DRNI: 0
  IGMPv3 specific queries: 0
  DRNI: 0
  IGMPv3 specific sg queries: 0
  DRNI: 0
  IGMPv1 reports: 0
  DRNI: 0
  IGMPv2 reports: 19
  DRNI: 19
  IGMPv3 reports: 0
  DRNI: 0
  IGMPv3 reports with right and wrong records: 0
  DRNI: 0
  IGMP leaves: 5
  DRNI: 5
  Error IGMP messages: 1
  DRNI: 1
Sent IGMP messages:
  IGMPv2 specific queries: 0
  IGMPv3 specific queries: 0
  IGMPv3 specific sg queries: 0
```



Received PIMv2 hello : 0

**Table 21 Command output**

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
error IGMP messages	Number of IGMP messages with errors.
DRNI	IGMP messages received on the DRNI IPP. NOTE: This field is supported in this version and later.

## Modified feature: Displaying statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping

### Feature change description

The layout of the command output was changed and support for displaying the number of MLD messages received on the DRNI IPP was added.

### Command changes

#### Modified command: display mld-snooping statistics

##### Syntax

```
display mld-snooping statistics
```

##### Views

Any view

##### Change description

Before modification: The **DRNI** field is not supported.

# Display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Sysname> display mld-snooping statistics
```

```
Received MLD general queries: 0
```

```
Received MLDv1 specific queries: 0
```

```
Received MLDv1 reports: 0
```

```
Received MLD done: 0
```

```
Sent MLDv1 specific queries: 0
```

```

Received MLDv2 reports: 0
Received MLDv2 reports with right and wrong records: 0
Received MLDv2 specific queries: 0
Received MLDv2 specific sg queries: 0
Sent MLDv2 specific queries: 0
Sent MLDv2 specific sg queries: 0
Received IPv6 PIM hello: 0
Received error MLD messages: 0

```

After modification: The **DRNI** field is supported.

# Display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Sysname> display mld-snooping statistics
```

Received MLD messages:

MLD general queries: 19

DRNI: 19

MLDv1 specific queries: 0

DRNI: 0

MLDv2 specific queries: 0

DRNI: 0

MLDv2 specific sg queries: 0

DRNI: 0

MLDv1 reports: 19

DRNI: 19

MLDv2 reports: 0

DRNI: 0

MLDv2 reports with right and wrong records: 0

DRNI: 0

MLD dones: 5

DRNI: 5

Error MLD messages: 1

DRNI: 1

Sent MLD messages:

MLDv1 specific queries: 0

MLDv2 specific queries: 0

MLDv2 specific sg queries: 0

Received IPv6 PIM hello: 0

**Table 22 Command output**

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
dones	Number of MLD done messages.
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.

error MLD messages	Number of MLD messages with errors.
DRNI	MLD messages received on the DRNI IPP. NOTE: This field is supported in this version and later.

## Modified feature: Enabling a VPN instance to replicate routes from the public network or other VPN instances

### Feature change description

This release allows a VPN instance to advertise the BGP routes replicated from the public network or another VPN instance.

### Command changes

#### Modified command: route-replicate

##### Old syntax

```
route-replicate from { public | vpn-instance vpn-instance-name } protocol
bgp as-number [ route-policy route-policy-name ]
```

##### New syntax

```
route-replicate from { public | vpn-instance vpn-instance-name } protocol
bgp as-number [ advertise ] [ route-policy route-policy-name ]
```

### Views

VPN instance IPv4 address family view

#### Change description

Before modification: The **advertise** keyword is not available when you enable a VPN instance to replicate BGP routes from the public network or another VPN instance.

After modification: The **advertise** keyword is available when you enable a VPN instance to replicate BGP routes from the public network or another VPN instance. This keyword allows the VPN instance to advertise the replicated BGP routes.

## Modified feature: Specifying outgoing labels for a static SRLSP

### Feature change description

From this release, the maximum number of outgoing labels that can be specified for a static SRLSP was changed to 4.

## Command changes

Modified command: `static-sr-mpls lsp`

### Syntax

```
static-sr-mpls lsp lsp-name out-label out-label-value&<1-n>
```

### Views

System view

### Change description

The value for the `n` argument was changed from 6 to 4.

## Modified feature: Creating an ACL

### Feature change description

This software version allows you to specify both a name and a number when creating an ACL.

## Command changes

Modified command: `acl`

### Old syntax

```
acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name } [ match-order { auto | config } ]  
acl mac { acl-number | name acl-name } [ match-order { auto | config } ]  
acl user-defined { acl-number | name acl-name }  
undo acl [ ipv6 ] { all | { advanced | basic } { acl-number | name acl-name } }  
undo acl mac { all | acl-number | name acl-name }  
undo acl user-defined { all | acl-number | name acl-name }
```

### New syntax

Command set 1:

```
acl [ ipv6 ] { name acl-name | number acl-number [ name acl-name ] [ match-order { auto | config } ] }  
undo acl [ ipv6 ] { all | name acl-name | number acl-number }
```

Command set 2:

```
acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name } [ match-order { auto | config } ]  
acl mac { acl-number | name acl-name } [ match-order { auto | config } ]  
acl user-defined { acl-number | name acl-name }  
undo acl [ ipv6 ] { all | { advanced | basic } { acl-number | name acl-name } }  
undo acl mac { all | acl-number | name acl-name }  
undo acl user-defined { all | acl-number | name acl-name }
```

## Views

System view

### Change description

Before modification: Command set 1 is not supported. You can create an ACL by specifying a name or a number, but not both. When creating a Layer 2 or user-defined ACL, you must specify the **mac** or **user-defined** keyword.

After modification: Command set 1 is supported. You can create an ACL by specifying both a name and a number. You can create a Layer 2 or user-defined ACL without specifying the **mac** or **user-defined** keyword.

## Modified feature: Referencing an ACL in QoS or packet filtering

### Feature change description

This software version allows you to reference a Layer 2 or user-defined ACL in QoS or packet filtering without specifying the **mac** or **user-defined** keyword..

## Command changes

Modified command: none

### Change description

The feature change applies to the following commands:

- **acl copy**
- **display acl**
- **display packet-filter statistics**
- **display packet-filter statistics sum**
- **display packet-filter verbose**
- **if-match acl**
- **packet-filter** (Ethernet service instance view)
- **packet-filter** (interface view)
- **packet-filter vlan-interface**
- **reset acl counter**
- **reset packet-filter statistics**

Before modification: When referencing a Layer 2 or user-defined ACL in QoS or packet filtering, you must specify the **mac** or **user-defined** keyword.

After modification: You can reference a Layer 2 or user-defined ACL without specifying the **mac** or **user-defined** keyword.

## Modified feature: Enabling hardware-count for the packet filtering default action

### Feature change description

In this release, this feature can be configured in Ethernet service instance view.

### Command changes

Modified command: packet-filter default hardware-count

#### Syntax

```
packet-filter default { inbound | outbound } hardware-count
undo packet-filter default { inbound | outbound } hardware-count
```

#### Views

Layer 2 Ethernet interface view  
Layer 2 aggregate interface view  
Layer 3 Ethernet interface view  
Layer 3 Ethernet subinterface view  
Layer 3 aggregate interface view  
VLAN interface view  
VSI interface view  
Ethernet service instance view

#### Change description

Before modification: The `packet-filter default hardware-count` command cannot be configured in Ethernet service instance view.

After modification: The `packet-filter default hardware-count` command can be configured in Ethernet service instance view.

## Modified feature: Configuring drop-level-based parameters for a queue in a WRED table

### Feature change description

This release added support for the `drop-level drop-level` option in the `undo` form of the command. You can restore the default for the command based on drop levels.

## Command changes

### Modified command: queue

#### Old syntax

```
queue queue-id [ drop-level drop-level ] low-limit low-limit high-limit  
high-limit [ discard-probability discard-prob ]  
undo queue { queue-id | all }
```

#### New syntax

```
queue queue-id [ drop-level drop-level ] low-limit low-limit high-limit  
high-limit [ discard-probability discard-prob ]  
undo queue { queue-id [ drop-level drop-level ] | all }
```

#### Views

WRED table view

#### Change description

Before modification: The **drop-level** *drop-level* option is not available in the **undo** form of the command.

After modification: The **drop-level** *drop-level* option is available in the **undo** form of the command.

## Modified feature: Configuring binding attributes for a local user

### Feature change description

Support of the binding interface attribute was added to device management users.

## Command changes

### Modified command: bind-attribute

#### Syntax

```
bind-attribute { ip ip-address | location interface interface-type  
interface-number | mac mac-address | vlan vlan-id } *
```

#### Views

Local user view

#### Change description

Before modification: The binding interface attribute is applicable only to network access users (LAN and portal users).

After modification: The binding interface attribute is applicable to both device management users and network access users (LAN and portal users).

# Modified feature: Password handling when global password control is enabled

## Feature change description

The following changes were added:

- The way that the device handles passwords of device management users when global password control is enabled.

Before modification:

- A password set in plaintext form is saved in encrypted form and a password set in hashed form is not saved.
- If a user changes its own password in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If the user changes its own password in hashed form, the system does not compare the new password with the current password or passwords in the history records.
- If a user deletes its own password, the system does not request the user to enter the current plaintext password.
- In FIPS mode, if a user with the network-admin user role changes its password, the system does not request the user to enter the current plaintext password.

After modification:

- All passwords in the history records are saved in hashed form.
- If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
- If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.
- If a user deletes its own password, the system requests the user to enter the current plaintext password.
- Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with passwords in the history records and the current password.

- The way the device handles super passwords when global password control is enabled:

Before modification:

- If a super new password is set in plaintext form, the password is saved in encrypted form. If a new super password is set in hashed form, the password is not saved.
- If a super password is changed in plaintext form, the new password must have a minimum of four characters different from the current password and any password in the history records. If a super password is changed in hashed form, the system does not compare the new password with the current password and passwords in the history records.

After modification:

- All super passwords in the history records are saved in hashed form.
- If a super password is changed in plaintext form, the new password must be different from all passwords in the history records and the current password. If a super password is changed in hashed form, the system does not compare the new password with the current one and those stored in the history password records.



## Command changes

None.

## Modified feature: Setting the quiet timer for RADIUS servers

### Feature change description

The minimum value of the RADIUS server quiet timer was changed from 1 minute to 0 minutes.

## Command changes

### Modified command: timer quiet (RADIUS scheme view)

#### Syntax

```
timer quiet minutes  
undo timer quiet
```

#### Views

RADIUS scheme view

#### Change description

Before modification: The value range for the *minutes* argument is 1 to 255 minutes.

After modification: The value range for the *minutes* argument is 0 to 255 minutes. If you set this argument to 0, the device does not change the state of the current server for a user when the server is unreachable. It sends an authentication or accounting request of the user to the next server in active state. For an authentication or accounting request of a new user, it still tries to send the request to the current server because the current server is in active state.

## Modified feature: Configuring MAC-based MAC authentication user accounts

### Feature change description

Support for password configuration was added to MAC-based MAC authentication user accounts.

## Command changes

### Modified command: mac-authentication user-name-format

#### Old syntax

```
mac-authentication user-name-format { fixed [ account name ] [ password  
{ cipher | simple } string ] | mac-address [ { with-hyphen | without-hyphen }  
[ lowercase | uppercase ] ] }
```

## New syntax

```
mac-authentication user-name-format { fixed [ account name ] | mac-address  
[ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] } [ password  
{ cipher | simple } string ]
```

## Views

System view

## Change description

Before modification: You cannot specify a password for MAC-based MAC authentication user accounts. The MAC address of each user is used as the password.

After modification: You can specify a password for all MAC-based MAC authentication user accounts by using the **password { cipher | simple } string** option. If you do not specify a password, each user uses its own MAC address as the password.

# Modified feature: MAC authentication VLAN mode

## Feature change description

As from this version, the device changes its manner in handling an online authenticated user that meets the following requirements:

- The user accesses a port in MAC authentication single-VLAN mode from a VLAN different from the VLAN where it was authenticated the last time.
- The user has been assigned an authorization VLAN.

## Command changes

### Modified command: mac-authentication host-mode

## Syntax

```
mac-authentication host-mode multi-vlan
```

## Views

Layer 2 Ethernet interface view

## Change description

As from this version, the device changes its manner in handling an online authenticated user that meets the following requirements:

- The user accesses a port in MAC authentication single-VLAN mode from a VLAN different from the VLAN where it was authenticated the last time.
- The user has been assigned an authorization VLAN.

Before modification: When the user accesses the port from a new VLAN, the device does not authenticate the user or log off the user from the authorization VLAN. The user is online in the authorization VLAN.

After modification: When the user accesses the port from a new VLAN, the device handles the user depending on the status of the port security MAC move feature.

- If port security MAC move is disabled, the user cannot pass authentication and come online from the new VLAN until after it goes offline from the port.

- If port security MAC move is enabled, the user can pass authentication on the new VLAN and come online without having to first go offline from the port. After the user passes authentication on the new VLAN, the original authentication session of the user is deleted from the port.

No changes were introduced to the command syntax.

---

**NOTE:**

To enable single-VLAN mode, execute the **undo** form of the **mac-authentication host-mode multi-vlan** command.

To enable the port security MAC move feature, use the **port-security mac-move permit** command.

---

## Modified feature: Port security MAC move

### Feature change description

As from this version, the port security MAC move feature takes effect on users that move between VLANs on a port in addition to users that move between ports.

### Command changes

#### Modified command: port-security mac-move permit

##### Syntax

```
port-security mac-move permit
```

##### Views

System view

##### Change description

Before modification: Port security MAC move setting takes effect only on users that move between ports on the device.

After modification: Port security MAC move setting also take effect on users that move between VLANs on a port in a VXLAN environment. In additional, user packets are VLAN tagged.

- If this feature is disabled, authenticated users must go offline from the original VLAN first before they can be reauthenticated successfully on the new VLAN and come online.
- If this feature is enabled, authenticated users can be reauthenticated successfully on the new VLAN without having to go offline from the original VLAN. The port will remove the users from the original VLAN immediately after the users are reauthenticated successfully on the new VLAN.

No changes were introduced to the command syntax.

---

**NOTE:**

MAC authentication multi-VLAN mode has higher priority than MAC move for users moving between VLANs on a port. If MAC authentication multi-VLAN mode is enabled, these users can come online in the new VLAN without being reauthenticated. To enable MAC authentication multi-VLAN mode, use the **mac-authentication host-mode multi-vlan** command.

---

# Modified feature: Web authentication support for HTTPS redirection

Before modification: Web authentication supports only HTTP redirection. It does not support HTTPS redirection.

After modification: Web authentication supports both HTTP redirection and HTTPS redirection. To redirect HTTPS requests of users, execute the `http-redirect https-port` command in system view to specify an HTTPS redirect listening port number.

## Modified feature: RSA key modulus length

### Feature change description

The supported RSA key modulus length was changed.

### Command changes

#### Modified command: public-key local create

##### Syntax

In non-FIPS mode:

```
public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1  
| secp521r1 ] | rsa } [ name key-name ]
```

In FIPS mode:

```
public-key local create { dsa | ecdsa [ secp256r1 | secp384r1 | secp521r1 ]  
| rsa } [ name key-name ]
```

##### Views

System view

##### Change description

Before modification, the key modulus length of a local RSA key pair is as follows:

- In non-FIPS mode:
  - Value range: 512 to 2048 bits.
  - Default: 1024 bits.To ensure security, use a minimum of 768 bits.
- In FIPS mode: 2048 bits.

After modification, the key modulus length of a local RSA key pair is as follows:

- In non-FIPS mode:
  - Value range: 512 to 4096 bits.
  - Default: 1024 bits.To ensure security, use a minimum of 768 bits.
- In FIPS mode:
  - Value range: A multiple of 256 bits in the range of 2048 to 4096 bits.
  - Default: 2048 bits.

# Modified feature: RSA key modulus length used for certification request in a PKI domain

## Feature change description

The value range for the RSA key modulus length used for certificate request in a PKI domain was changed.

## Command changes

Modified command: public-key rsa

### Syntax

```
public-key rsa { { encryption name encryption-key-name [ length key-length ]  
| signature name signature-key-name [ length key-length ] } * | general name  
key-name [ length key-length ] }
```

### Views

PKI domain view

### Feature change description

Before modification:

- In non-FIPS mode, the value range for the *key-length* argument is 512 to 2048 bits, and the default is 1024 bits.
- In FIPS mode, the value for the *key-length* argument must be 2048 bits.

After modification:

- In non-FIPS mode, the value range for the *key-length* argument is 512 to 4096 bits, and the default is 1024 bits.
- In FIPS mode, the value for the *key-length* argument must be a multiple of 256 in the range of 2048 to 4096, and the default is 2048.

# Modified feature: Displaying IPv4SG bindings

## Feature change description

This feature has the following changes:

- Support for displaying IPv4SG bindings generated based on ARP snooping for VLANs was added.
- Support for displaying IPv4SG bindings generated based on ARP snooping for VSIs was added.
- Support for display IPv4SG bindings generated based on the ARP flood suppression module was removed.

## Command changes

Modified command: display ip source binding

### Old syntax

```
display ip source binding [ static | [ vpn-instance vpn-instance-name ]  
[ arp-snooping | arp-suppression | dhcp-relay | dhcp-server | dhcp-snooping  
| dot1x ] ] [ ip-address ip-address ] [ mac-address mac-address ] [ vlan  
vlan-id ] [ interface interface-type interface-number ] [ slot  
slot-number ]
```

### New syntax

```
display ip source binding [ static | [ vpn-instance vpn-instance-name ]  
[ arp-snooping-vlan | arp-snooping-vsi | dhcp-relay | dhcp-server |  
dhcp-snooping | dot1x ] ] [ ip-address ip-address ] [ mac-address  
mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ]  
[ slot slot-number ]
```

### Views

Any view

### Change description

The **arp-snooping** keyword was changed to the **arp-snooping-vlan** and **arp-snooping-vsi** keywords, and the **arp-suppression** keyword was removed

**arp-snooping-vlan**: Specifies IPv4SG bindings generated based on ARP snooping for VLANs.

**arp-snooping-vsi**: Specifies IPv4SG bindings generated based on ARP snooping for VSIs.

## Modified feature: Displaying IPv6SG bindings

### Feature change description

This feature has the following changes:

- Support for displaying IPv6SG bindings generated based on ND snooping for VLANs was added.
- Support for displaying IPv6SG bindings generated based on ND snooping for VSIs was added.
- Support for display IPv6SG bindings generated based on the ND flood suppression module was removed.

## Command changes

Modified command: display ipv6 source binding

### Old syntax

```
display ipv6 source binding [ static | [ vpn-instance vpn-instance-name ]  
[ dhcpv6-relay | dhcpv6-snooping | dot1x | nd-snooping ] ] [ ip-address  
ipv6-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface  
interface-type interface-number ] [ slot slot-number ]
```

## New syntax

```
display ipv6 source binding [ static | [ vpn-instance vpn-instance-name ]  
[ dhcpv6-relay | dhcpv6-server | dhcpv6-snooping | dot1x |  
nd-snooping-vlan | nd-snooping-vsi ] ] [ ip-address ipv6-address ]  
[ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type  
interface-number ] [ slot slot-number ]
```

## Views

Any view

## Change description

The **nd-snooping** keyword was changed to the **nd-snooping-vlan** and **nd-snooping-vsi** keywords, and the **arp-suppression** keyword was removed

**nd-snooping-vlan**: Specifies IPv6SG bindings generated based on ND snooping for VLANs.

**nd-snooping-vsi**: Specifies IPv6SG bindings generated based on ND snooping for VSIs.

# Modified feature: Displaying the MFF configuration for a VLAN

## Feature change description

From this release, the **display mac-forced-forwarding vlan** command does not support displaying the MFF operating mode.

## Command changes

### Modified command: display mac-forced-forwarding vlan

#### Syntax

```
display mac-forced-forwarding vlan vlan-id
```

#### Views

Any view

#### Predefined user roles

network-admin

network-operator

#### Change description

Before modification: The MFF operating mode is displayed in the command output.

# Display the MFF configuration for VLAN 2.

```
<Sysname> display mac-forced-forwarding vlan 2
```

```
VLAN 2
```

```
Mode: Manual/Single
```

```
Gateway:
```

```
-----  
192.168.1.42          000f-e200-8046
```

```
Server:
```

```
-----
```

192.168.1.48

192.168.1.49

**Table 5 Command output**

Field	Description
VLAN 2	ID of the VLAN to which the gateways belong.
Mode	MFF operating mode: <ul style="list-style-type: none"><li>• <b>Manual</b>—Manual mode.</li><li>• <b>Single</b>—Single-gateway mode.</li></ul>
Gateway	IP and MAC addresses of gateways. If no address is learned, this field displays <b>N/A</b> .
Server	Server IP addresses.

After modification: The command does not support displaying the MFF operating mode.

# Display the MFF configuration for VLAN 2.

```
<Sysname> display mac-forced-forwarding vlan 2
```

VLAN 2

Gateway:

-----

192.168.1.42                      000f-e200-8046

Server:

-----

192.168.1.48                      192.168.1.49

**Table 6 Command output**

Field	Description
VLAN 2	ID of the VLAN to which the gateways belong.
Gateway	IP and MAC addresses of gateways. If no address is learned, this field displays <b>N/A</b> .
Server	Server IP addresses.

## Modified feature: Associating Track with application modules

### Feature change description

From this release, you cannot configure the notification delay when associating Track with application modules. Creating a track entry associated with an application module enters Track view. You can configure the delay only in Track view for notifying the application module of track entry state changes.

### Command changes

#### Modified command: track bfd ctrl

##### Old syntax

```
track track-entry-number bfd ctrl [ interface interface-type interface-number  
| vpn-instance vpn-instance-name ] remote ip remote-ip-address local ip
```



```
local-ip-address [ delay { negative negative-time | positive positive-time }  
* ]
```

### New syntax

```
track track-entry-number bfd ctrl [ interface interface-type  
interface-number | vpn-instance vpn-instance-name ] remote ip  
remote-ip-address local ip local-ip-address
```

### Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track bfd echo

### Old syntax

```
track track-entry-number bfd echo interface interface-type interface-number  
remote ip remote-ip-address local ip local-ip-address [ delay { negative  
negative-time | positive positive-time } * ]
```

### New syntax

```
track track-entry-number bfd echo interface interface-type  
interface-number remote ip remote-ip-address local ip local-ip-address
```

### Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track cfd

### Old syntax

```
track track-entry-number cfd cc service-instance instance-id mep mep-id  
[ delay { negative negative-time | positive positive-time } * ]
```

### New syntax

```
track track-entry-number cfd cc service-instance instance-id mep mep-id
```

### Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track interface

### Old syntax

```
track track-entry-number interface interface-type interface-number [ delay  
{ negative negative-time | positive positive-time } * ]
```

## New syntax

```
track track-entry-number interface interface-type interface-number
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track interface physical

### Old syntax

```
track track-entry-number interface interface-type interface-number physical  
[ delay { negative negative-time | positive positive-time } * ]
```

### New syntax

```
track track-entry-number interface interface-type interface-number  
physical
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track interface protocol

### Old syntax

```
track track-entry-number interface interface-type interface-number protocol  
{ ipv4 | ipv6 } [ delay { negative negative-time | positive positive-time } * ]
```

### New syntax

```
track track-entry-number interface interface-type interface-number  
protocol { ipv4 | ipv6 }
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track ip route reachability

### Old syntax

```
track track-entry-number ip route [ vpn-instance vpn-instance-name ]  
ip-address { mask-length | mask } reachability [ delay { negative negative-time  
| positive positive-time } * ]
```

### New syntax

```
track track-entry-number ip route [ vpn-instance vpn-instance-name ]  
ip-address { mask-length | mask } reachability
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track lldp neighbor

### Old syntax

```
track track-entry-number lldp neighbor interface interface-type  
interface-number [ delay { negative negative-time | positive positive-time }  
* ]
```

### New syntax

```
track track-entry-number lldp neighbor interface interface-type  
interface-number
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified command: track nqa

### Old syntax

```
track track-entry-number nqa entry admin-name operation-tag reaction  
item-number [ delay { negative negative-time | positive positive-time } * ]
```

### New syntax

```
track track-entry-number nqa entry admin-name operation-tag reaction  
item-number
```

## Change description

Before modification: This command allows you to set the notification delay when associating Track with the application module, and does not enter Track view.

After modification: Creating a track entry associated with the application module enters Track view. You can configure the notification delay in Track view.

## Modified feature: Specifying the length of ICMP echo requests sent by an IPv4 or IPv6 ping operation

## Feature change description

The maximum length of ICMP echo requests that can be sent by an IPv4 or IPv6 ping operation was changed from 8100 bytes to 9600 bytes.

## Command changes

### Modified command: ping

#### Syntax

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type  
interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t  
timeout | -tos tos | -v | -vpn-instance vpn-instance-name ] * host
```

#### Views

Any view

#### Change description

Before modification: The value range for the *packet-size* argument is 20 to 8100 bytes.

After modification: The value range for the *packet-size* argument is 20 to 9600 bytes.

### Modified command: ping ipv6

#### Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -i interface-type interface-number  
| -m interval | -q | -s packet-size | -t timeout | -tc traffic-class | -v  
| -vpn-instance vpn-instance-name ] * host
```

#### Views

Any view

#### Change description

Before modification: The value range for the *packet-size* argument is 20 to 8100 bytes.

After modification: The value range for the *packet-size* argument is 20 to 9600 bytes.

## Modified feature: Removing a TCP or UDP listening service for a VPN instance

### Feature change description

From this release, you can remove a TCP or UDP listening service for the specified VPN instance.

## Command changes

### Modified command: nqa server tcp-connect

#### Old syntax

```
nqa server tcp-connect ip-address port-number [ vpn-instance  
vpn-instance-name ] [ tos tos ]  
  
undo nqa server tcp-connect ip-address port-number
```

#### New syntax

```
nqa server tcp-connect ip-address port-number [ vpn-instance  
vpn-instance-name ] [ tos tos ]
```

```
undo nqa server tcp-connect ip-address port-number [ vpn-instance
vpn-instance-name ]
```

## Views

System view

## Change description

The **vpn-instance** *vpn-instance-name* option was added to the **undo** form of the command.

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens to the TCP services on an IP address on the public network.

Modified command: nqa server udp-echo

## Old syntax

```
nqa server udp-echo ip-address port-number [ vpn-instance
vpn-instance-name ] [ tos tos ]
```

```
undo nqa server udp-echo ip-address port-number
```

## New syntax

```
nqa server udp-echo ip-address port-number [ vpn-instance
vpn-instance-name ] [ tos tos ]
```

```
undo nqa server udp-echo ip-address port-number [ vpn-instance
vpn-instance-name ]
```

## Views

System view

## Change description

The **vpn-instance** *vpn-instance-name* option was added to the **undo** form of the command.

**vpn-instance** *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the NQA server listens to UDP services on an IP address on the public network.

# Modified feature: Specifying the source IP address for NTP messages

## Feature change description

You can configure the source IP address for NTP messages directly or by specifying an interface. Before the modification, the source IP address can be configured only by specifying an interface.

## Command changes

Modified command: ntp-service source

## Old syntax

```
ntp-service source interface-type interface-number
```

## New syntax

```
ntp-service source { interface-type interface-number | ip-address }
```

## Views

System view

## Parameter

*interface-type interface-number*: Specifies an interface by its type and number. The device uses the primary address of the specified source interface as the source address to send NTP messages. The destination address of the NTP response messages is the primary address of the specified source interface.

*ip-address*: Specifies the source IP address for NTP messages.

## Change description

The *ip-address* argument was added to the command.

# New feature: Specifying the NTP time-offset thresholds for log and trap outputs

## Specifying the NTP time-offset thresholds for log and trap outputs

### About the NTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the NTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

### Procedure

1. Enter system view.  
**system-view**
2. Specify the NTP time-offset thresholds for log and trap outputs.  
**ntp-service time-offset-threshold { log log-threshold | trap trap-threshold } \***  
By default, no NTP time-offset thresholds are set for log and trap outputs.

## Command reference

### ntp-service time-offset-threshold

Use **ntp-service time-offset-threshold** to set the NTP time-offset thresholds for log and trap outputs.

Use **undo ntp-service time-offset-threshold** to restore the default.

### Syntax

```
ntp-service time-offset-threshold { log log-threshold | trap trap-threshold } *  
undo ntp-service time-offset-threshold
```

## Default

No NTP time-offset thresholds are set for log and trap outputs.

## Views

System view

## Predefined user roles

network-admin

mdc-admin

## Parameters

**log** *log-threshold*: Specifies the NTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

**trap** *trap-threshold*: Specifies the NTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

## Usage guidelines

By default, the system synchronizes the NTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

## Examples

# Set the NTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
```

```
[Sysname] ntp-service time-offset-threshold log 500 trap 600
```

# New feature: Specifying the SNTP time-offset thresholds for log and trap outputs

## Specifying the SNTP time-offset thresholds for log and trap outputs

### About SNTP time-offset thresholds for log and trap outputs

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the SNTP time-offset thresholds for log and trap outputs, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

## Procedure

1. Enter system view.

```
system-view
```

2. Specify the SNTP time-offset thresholds for log and trap outputs.

```
sntp time-offset-threshold { log log-threshold | trap trap-threshold }  
*
```

By default, no SNTP time-offset thresholds are set for log and trap outputs

## Command reference

### sntp time-offset-threshold

Use **sntp time-offset-threshold** to specify the SNTP time-offset thresholds for log and trap outputs.

Use **undo sntp time-offset-threshold** to restore the default.

#### Syntax

```
sntp time-offset-threshold { log log-threshold | trap trap-threshold } *  
undo sntp time-offset-threshold
```

#### Default

No SNTP time-offset thresholds are set for log and trap outputs.

#### Views

System view

#### Predefined user roles

network-admin

mdc-admin

#### Parameters

**log** *log-threshold*: Specifies the SNTP time-offset threshold for log output. The value range for the *log-threshold* argument is 128 to 60000, in milliseconds.

**trap** *trap-threshold*: Specifies the SNTP time-offset threshold for trap output. The value range for the *trap-threshold* argument is 128 to 60000, in milliseconds.

#### Usage guidelines

By default, the system synchronizes the SNTP client's time to the server and outputs a log and a trap when the time offset exceeds 128 ms for multiple times.

After you set the thresholds, the system synchronizes the client's time to the server when the time offset exceeds 128 ms for multiple times, but outputs logs and traps only when the time offset exceeds the specified thresholds, respectively.

#### Examples

# Set the SNTP time-offset thresholds for log and trap outputs to 500 ms and 600 ms, respectively.

```
<Sysname> system-view
```

```
[Sysname] sntp time-offset-threshold log 500 trap 600
```

## Modified feature: Creating a sampler

### Feature change description

The value range for the sampling rate of a sampler was modified.



## Command changes

Modified command: `sampler`

### Syntax

```
sampler sampler-name mode random packet-interval n-power rate
```

### Views

System view

### Change description

Before modification: The value range for the *rate* argument is 1 to 13.

After modification: The value range for the *rate* argument is 0 to 13.

## Modified feature: sFlow counter sampling

### Feature change description

In this version and later, you can specify an sFlow instance for counter sampling.

## Command changes

Modified command: `sflow counter collector`

### Old syntax

```
sflow counter collector collector-id  
undo sflow counter collector
```

### New syntax

```
sflow counter [ instance instance-id ] collector collector-id  
undo sflow counter [ instance instance-id ] collector
```

### Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

### Parameters

**instance** *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for counter sampling.

### Change description

Before modification: You can specify only an sFlow collector for counter sampling.

After modification: You can specify an sFlow instance and an sFlow collector for counter sampling.

## Modified feature: sFlow flow sampling

### Feature change description

In this version and later, you can specify an sFlow instance for flow sampling.

### Command changes

Modified command: sflow counter collector

#### Old syntax

```
sflow flow collector collector-id  
undo sflow flow collector
```

#### New syntax

```
sflow flow [ instance instance-id ] collector collector-id  
undo sflow flow [ instance instance-id ] collector
```

#### Views

Layer 2 Ethernet interface view  
Layer 3 Ethernet interface view

#### Parameters

**instance** *instance-id*: Specifies an sFlow instance by its ID in the range of 1 to 4. The default ID for an sFlow instance is 1. If you do not specify an sFlow instance, this command specifies sFlow instance 1 for flow sampling.

#### Change description

Before modification: You can specify only an sFlow collector for flow sampling.

After modification: You can specify an sFlow instance and an sFlow collector for flow sampling.

## Modified feature: Configuring a backup PW for a cross-connect

### Feature change description

The value range for the outgoing label of a backup PW was changed.

### Command changes

Modified command: backup-peer

#### Syntax

```
backup-peer ip-address pw-id pw-id [ in-label label-value out-label label-value ] [ pw-class class-name | tunnel-policy tunnel-policy-name ] *
```

#### Views

Cross-connect PW view

## Change description

Before modification: The value range for the outgoing label of a backup PW is 16 to 1023.

After modification: The value range for the outgoing label of a backup PW is 16 to 1048575.

# Modified feature: Configuring a backup PW for a VSI

## Feature change description

The value range for the outgoing label of a backup PW was modified.

## Command changes

Modified command: `backup-peer`

### Syntax

In VSI LDP PW view:

```
backup-peer ip-address [ pw-id pw-id ] [ pw-class class-name | tunnel-policy tunnel-policy-name ] *
```

In VSI static PW view:

```
backup-peer ip-address [ pw-id pw-id ] in-label label-value out-label label-value [ pw-class class-name | tunnel-policy tunnel-policy-name ] *
```

### Views

VSI LDP PW view

VSI static PW view

## Change description

Before modification: The value range for the outgoing label of a backup PW is 16 to 1023.

After modification: The value range for the outgoing label of a backup PW is 16 to 1048575.

# Modified feature: Change of the bandwidth limit value range for VSIs

## Feature change description

The value range for the VSI bandwidth limit was changed.

## Command changes

Modified command: `bandwidth`

### Syntax

```
bandwidth bandwidth
```

```
undo bandwidth
```

## Views

VSI view

## Change description

Before modification: The value range for the *bandwidth* argument is 64 to 4194303 kbps.

After modification: The value range for the *bandwidth* argument is 64 to 167772159 kbps.

# Modified feature: Value range change for the broadcast, multicast, or unknown unicast restraint bandwidth of VSIs

## Feature change description

The value range for the broadcast, multicast, or unknown unicast restraint bandwidth of VSIs was changed.

## Command changes

Modified command: `restrain`

### Syntax

```
restrain { broadcast | multicast | unknown-unicast } bandwidth
undo restrain { broadcast | multicast | unknown-unicast }
```

## Views

VSI view

## Change description

Before modification: The value for the *bandwidth* argument can be 0 or in the range of 64 to 4194303 kbps.

After modification: The value for the *bandwidth* argument can be 0 or in the range of 64 to 167772159 kbps.

# Modified feature: Frame match criteria of VXLAN Ethernet service instances

## Feature change description

The frame match criteria were changed for Ethernet service instances in VLAN access mode.

## Command changes

Modified command: `encapsulation`

### Syntax

```
encapsulation s-vid vlan-id [ c-vid { vlan-id-list | all } | only-tagged ]
```

```

encapsulation s-vid vlan-id-list [ c-vid vlan-id-list ]
encapsulation { default | tagged | untagged }
undo encapsulation

```

## Views

Ethernet service instance view

## Change description

Before modification: On a Layer 2 Ethernet or aggregate interface, if you configure the **encapsulation default** criterion for an Ethernet service instance in VLAN access mode, make sure no other Ethernet service instances exist on the interface.

After modification: On a Layer 2 Ethernet or aggregate interface, if an Ethernet service instance in VLAN access mode uses the **encapsulation default** criterion, you can create other Ethernet service instances on the interface. The interface matches traffic to the Ethernet service instances in the following criterion order:

- **encapsulation { tagged | untagged }**
- **encapsulation default**
- **encapsulation s-vid vlan-id [ c-vid { vlan-id | all } | only-tagged ]** and **encapsulation s-vid vlan-id-list [ c-vid vlan-id-list ]**

# Modified feature: Displaying EVPN routing table information

## Feature change description

ECMP route flags were added to the output from the **display evpn routing-table** command.

## Command changes

### Modified command: display evpn routing-table

#### Syntax

```

display evpn routing-table [ ipv6 ] { public-instance | vpn-instance
vpn-instance-name } [ count ]

```

## Views

Any view

## Change description

The **Flags** field was added to the command output to display ECMP route flags.

- **E**—The route carries a valid ESI.
- **A**—All Ethernet auto-discovery routes are received. The ECMP routes for the next hop can be issued.
- **L**—An active local ESI exists. Remote routes are not issued.
- **—**—The MAC/IP advertisement route does not have a valid ESI. ECMP routes are not supported.

## Modified feature: NETCONF logging

### Feature change description

The default setting for NETCONF logging was changed.

Before modification: NETCONF logging is disabled.

After modification: NETCONF logging is enabled only for row operations for <action> and <edit-config> operations.

### Command changes

#### Modified command: netconf log

##### Old syntax

```
netconf log source { all | { agent | soap } * } { protocol-operation { all  
| { action | config | get | set | session | syntax | others } * } |  
row-operation | verbose }  
  
undo netconf log source { all | { agent | soap } * } { protocol-operation  
{ all | { action | config | get | session | set | syntax | others } * }  
| row-operation | verbose }
```

##### New syntax

```
netconf log source { all | { agent | soap } * } { protocol-operation { all  
| { action | config | get | set | session | syntax | others } * } | verbose }  
  
undo netconf log source { all | { agent | soap } * } { protocol-operation  
{ all | { action | config | get | session | set | syntax | others } * }  
| verbose }
```

##### Views

System view

##### Change description

Before modification: NETCONF logging is disabled by default. To enable the device to log row operations for <action> and <edit-config> operations, you must execute the **netconf log source { all | { agent | soap } \* } protocol-operation** command.

After modification: NETCONF logging is enabled only for row operations of <action> and <edit-config> operations by default. You do not need to execute the **netconf log source { all | { agent | soap } \* } protocol-operation** command.

## Modified feature: Specifying the role of the device in the VCF fabric

### Feature change description

In this version and later, a data center VCF fabric supports the spine-aggregate-leaf topology. Residing on the distribution layer, an aggregate node is between leaf nodes and spine nodes. In such a VCF fabric, OSPF runs on the Layer 3 networks between the spine and aggregate nodes and between the aggregate and leaf nodes. The default role of the device in the VCF fabric is aggregate.

Automated overlay network deployment is not supported on aggregate nodes.

## Command reference

### Modified command: vcf-fabric role

#### Old syntax

```
vcf-fabric role { access | leaf | spine }  
undo vcf-fabric role
```

#### New syntax

```
vcf-fabric role { access | aggr | leaf | spine }  
undo vcf-fabric role
```

#### Views

System view

#### Change description

The **aggr** keyword was added. The default role of the device in the VCF fabric was changed to aggregate.

**aggr**: Specifies the aggregate node.

### Modified command: display vcf-fabric role

#### Syntax

```
display vcf-fabric role
```

#### Views

Any view

#### Change description

The **aggr** value was added to the **Default role** and **Current role** fields.

Before modification:

# Display the role of the device in the VCF fabric.

```
<System> display vcf-fabric role
```

```
Default role: leaf
```

```
Current role: leaf
```

After modification:

# Display the role of the device in the VCF fabric.

```
<System> display vcf-fabric role
```

```
Default role: aggr
```

```
Current role: aggr
```

**Table 23 Command output**

Field	description
Default role	Default role of the device in the VCF fabric: <ul style="list-style-type: none"><li><b>spine</b>—The device is a spine node.</li><li><b>aggr</b>—The device is an aggregate node.</li><li><b>leaf</b>—The device is a leaf node.</li></ul>

Field	description
	<ul style="list-style-type: none"> <li><b>access</b>—The device is an access node.</li> </ul> <p><b>NOTE:</b> The <b>aggr</b> value was added in this version.</p>
Current role	<p>Current role of the device in the VCF fabric:</p> <ul style="list-style-type: none"> <li><b>spine</b>—The device is a spine node.</li> <li><b>aggr</b>—The device is an aggregate node.</li> <li><b>leaf</b>—The device is a leaf node.</li> <li><b>access</b>—The device is an access node.</li> </ul> <p><b>NOTE:</b> The <b>aggr</b> value was added in this version.</p>

## Related commands

`vcf-fabric role`

## Modified command: display vcf-fabric underlay autoconfigure

### Syntax

`display vcf-fabric underlay autoconfigure`

### Views

Any view

### Change description

Before modification: VCF fabric does not support the spine-aggregate-leaf topology.

After modification: VCF fabric supports the spine-aggregate-leaf topology. If you use this command on a master spine node, BGP peer information on all spine and leaf nodes will be displayed.

**# Display information about automated underlay network deployment.**

```
<Sysname> display vcf-fabric underlay autoconfigure
```

success command:

```
#
system
clock timezone beijing add 08:00:00
#
system
lldp global enable
lldp compliance cdp
#
system
ospf 1
graceful-restart ietf
area 0.0.0.0
#
system
interface LoopBack0
#
system
l2vpn enable
```



```

#
system
vxlan tunnel mac-learning disable
vxlan tunnel arp-learning disable
#
system
stp global enable
#
system
ntp-service enable
ntp-service unicast-peer 172.16.1.136
#
system
netconf soap https enable
restful https enable
#
system
info-center loghost 172.16.1.136
#
system
local-user aaa
password *****
service-type https
authorization-attribute user-role network-admin
#
system
line vty 0 63
authentication-mode scheme
user-role network-admin
#
system
bgp 100
graceful-restart
address-family l2vpn evpn
#
system
vcf-fabric topology enable
#
system
neutron
rabbit user openstack
rabbit password *****
rabbit host ip 172.16.1.136
restful user aaa password *****
vpn-target 1:1 export-extcommunity
vsi-mac 789c-2f5f-0200
network-type distributed-vxlan
proxy-arp enable

```

```

    l2agent enable
    l3agent enable
#
    system
    snmp-agent
    snmp-agent packet max-size 4096
    snmp-agent community read public
    snmp-agent community write private
    snmp-agent sys-info version all
#
Uplink interface:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
Downlink interface:
    Ten-GigabitEthernet1/0/3
    Ten-GigabitEthernet1/0/4
Loopback0 IP allocation:


| Device_MAC     | Loopback_IP | Management_IP | State |
|----------------|-------------|---------------|-------|
| a43c-adae-0400 | 200.1.1.6   | 172.16.1.193  | Up    |
| a43c-9aa7-0100 | 200.1.1.4   | 172.16.1.152  | Up    |


Loopback1 IP allocation:


| Device_MAC     | Loopback_IP | Management_IP | State |
|----------------|-------------|---------------|-------|
| a43c-adae-0400 | 100.1.1.6   | 172.16.1.193  | Up    |
| a43c-9aa7-0100 | 100.1.1.4   | 172.16.1.152  | Up    |


Aggregation configuration:
    AggrID: 7
    interface: Ten-GigabitEthernet1/0/5
    interface: Ten-GigabitEthernet1/0/6
IRF allocation:
    Self Bridge Mac: a43c-adae-0400
    IRF Status: Yes
    Member List: [1, 2]
BGP peer configuration:
    Device_MAC: 265b-208d-0300
    Device_role:leaf
    BGP peer list:
        200.1.4.5
    Device_MAC: 1ea6-06a4-0500
    Device_role:spine
    BGP peer list:
        200.1.4.4
        200.1.4.7
    Device_MAC: 1ead-aed1-0600
    Device_role:leaf
    BGP peer list:
        200.1.4.5

```

**Table 24 Command output**

Field	Description
success command	Commands that have been successfully executed during automated underlay network deployment.
Uplink interface	Uplink interfaces of the device.
Downlink interface	Downlink interfaces of the device.
Loopback0 IP allocation	IP addresses assigned to Loopback 0.
Loopback1 IP allocation	IP addresses assigned to Loopback 1.
Aggregation configurations	Information about Layer 2 aggregation groups.
IRF allocation	IRF configurations, including IRF bridge MAC address of the IRF fabric, IRF status, and the IRF member ID of the device.
BGP peer configuration	<p>Information about BGP peers of the device.</p> <p><b>NOTE:</b></p> <p>In this version and later, BGP peer information on all spine and leaf nodes is displayed only when this command is executed on the master spine node in a spine-aggregate-leaf VCF fabric.</p>