



Hewlett Packard
Enterprise

5140HI-CMW710-R6652P05 Release Notes

Contents

Introduction.....	1
Version information.....	1
Version number.....	1
Version history	1
Hardware and software compatibility matrix	2
ISSU upgrade type matrix.....	3
Upgrade advice.....	3
Upgrade restrictions and guidelines.....	3
Hardware feature updates	4
R6652P05~R6628P40	4
R6628P35	4
R6615P07	4
R6615P06	4
Software feature and command updates	4
MIB updates	4
Operation changes	4
Operation changes in R6652P05~R6628P40.....	4
Operation changes in R6628P35.....	5
Operation changes in R6615P07	5
Operation changes in R6615P06.....	5
Restrictions and cautions.....	5
Restrictions	5
Cautions.....	6
Open problems and workarounds	6
List of resolved problems	6
Resolved problems in R6652P05	6
Resolved problems in R6628P47	8
Resolved problems in R6628P43	10
Resolved problems in R6628P40	11
Resolved problems in R6628P35	16
Resolved problems in R6615P07	23
Resolved problems in R6615P06	26
Support and other resources	26
Accessing Hewlett Packard Enterprise Support.....	26
Documents	27

Related documents	27
Documentation feedback	28
Appendix A Feature list.....	29
Hardware features.....	29
Software features.....	32
Appendix B Fixed security vulnerabilities	35
Fixed security vulnerabilities in R6652P05	35
Fixed security vulnerabilities in R6628P35	41
Fixed security vulnerabilities in R6615P07	42
Appendix C Upgrading software	43
System software file types	43
System startup process.....	43
Upgrade methods.....	44
Upgrading from the CLI.....	45
Preparing for the upgrade	45
Downloading software images to the master switch	46
Upgrading the software images	48
Upgrading from the Boot menu.....	50
Prerequisites	50
Accessing the Boot menu	51
Accessing the basic Boot menu	52
Accessing the extended Boot menu.....	53
Upgrading Comware images from the Boot menu	54
Upgrading Boot ROM from the Boot menu	62
Managing files from the Boot menu	69
Handling software upgrade failures.....	72

List of tables

Table 1 Version history	1
Table 2 Hardware and software compatibility matrix	2
Table 3 ISSU version compatibility matrix.....	3
Table 4 MIB updates	4
Table 5 5140HI series hardware features for non-PoE switch models	29
Table 6 5140HI series hardware features for PoE switch models	30
Table 7 PoE power capacity of the HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw Swch switches	31
Table 8 Software features of the 5140HI series.....	32
Table 9 Minimum free storage space requirements.....	50
Table 10 Shortcut keys	51
Table 11 Basic Boot ROM menu options.....	52
Table 12 BASIC ASSISTANT menu options.....	52
Table 13 Extended Boot ROM menu options.....	53
Table 14 EXTENDED ASSISTANT menu options	54
Table 15 TFTP parameter description	55
Table 16 FTP parameter description.....	56
Table 17 TFTP parameter description	63
Table 18 FTP parameter description.....	64

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 5140HI-CMW710-R6652P05. 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 the documents listed in "[Related documents](#)."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 6652P05.

NOTE:

To identify the version number (see Note①), execute the **display version** command in any view.

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
R6652P05	R6628P47	2024-03-31	Release version	None
R6628P47	R6628P43	2023-12-29	Release version	None
R6628P43	R6628P40	2023-08-21	Release version	None
R6628P40	R6628P35	2023-07-15	Release version	None
R6628P35	R6615P07	2023-4-25	Release version	None
R6615P07	R6615P06	2022-06-09	Release version	None
R6615P06	First release	2022-03-25	Release version	First release

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	5140HI Series
Hardware platform	HPE 5140 24G 4SFP+ 1-slot HI Swch HPE 5140 48G 4SFP+ 1-slot HI Sw HPE 5140 24G PoE+ 4SFP+ 1-slot HI Sw HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw HPE 5140/5520 10GBASE-T MACsec 2p Mod
Minimum memory requirements	2GB
Minimum Flash requirements	512 M
Boot ROM version	Version 119 or higher (Note: Use the display version command in any view to view the version information. Please see Note②)
Host software	5140HI-CMW710-R6652P05.ipe (See the MD5 file)
iMC version	iMC ACLM 7.3 (E0705P12) iMC PLAT 7.3 (E0705P12) iMC QoS 7.3(E0505P01) iMC EIA 7.3 (E0611P13) iMC NTA 7.3 (E0707P06) iMC SHM 7.3 (E0707L06) iMC EAD 7.3 (E0611P10) iMC ICC 7.3 (E0705P12) iMC VLAN 7.3 (E0705P12)
iNode version	iNode 7.3 (E0585)
Remarks	None

Display the system software and Boot ROM versions of 5140HI

```
<Sysname>display version
```

HPE Comware Software, Version 7.1.070, Release 6615P07 -----Note①

Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP

HPE 5520 24G 4SFP+ HI Swch R8M25A uptime is 0 weeks, 0 days, 0 hours, 8 minutes

Last reboot reason : User reboot

Boot image: flash:/5140HI-cmw710-boot-r6615P07.bin

Boot image version: 7.1.070, Release 6615P07

Compiled Jun 16 2021 11:00:00

System image: flash:/5140HI-cmw710-system-r6615P07.bin

System image version: 7.1.070, Release 6615P07

```

Compiled Jun 16 2021 11:00:00
Feature image(s) list:
  flash:/5140HI-cmw710-freeradius-r6615P07.bin, version: 7.1.070, Release 6615P07
    Compiled Jun 16 2021 11:00:00
  flash:/5140HI-cmw710-escan-r6615P07.bin, version: 7.1.070, Release 6615P07
    Compiled Jun 16 2021 11:00:00

Slot 1:
Uptime is 0 weeks,0 days,0 hours,8 minutes
5520 24G 4SFP+ HI Swch with 2 Processors
BOARD TYPE:          5520 24G 4SFP+ HI Swch
DRAM:                2048M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.B
Bootrom Version:    119          -----Note②
CPLD 1 Version:      001
Release Version:     HPE 5520 24G 4SFP+ HI Swch R8M26A-6615P07
Patch Version  :     None
Reboot Cause  :      UserReboot
[SubSlot 0] 48GE+4SFP Plus

```

ISSU upgrade type matrix

ISSU provides compatible upgrade and incompatible upgrade, depending on the compatibility between software versions. [Table 3](#) provides the approved ISSU upgrade types only between the current version and the history versions within the past 18 months. This matrix does not include history versions that are 18 months earlier than the current version, for which, no ISSU upgrade verification was performed.

For more information about ISSU, see the fundamentals configuration guide for the device.

Table 3 ISSU version compatibility matrix

Current version	History version	ISSU upgrade method
5140HI-CMW710-R6652P05	5140HI-CMW710-R6628P47	Incompatible

Upgrade advice

Upgrade to this version as needed to gain benefits introduced in this version.

Upgrade restrictions and guidelines

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.

Hardware feature updates

R6652P05~R6628P40

None

R6628P35

Supported HPE 5140/5520/5600 4P BASE-T/6P SFP Mod, HPE 5140/5520/5600 4P 1/10G SFP+ Mod and HPE 5140/5520/5600 2P SFP28 Mod.

R6615P07

None

R6615P06

First release

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5140HI-CMW710-R6652P05 Release Notes (Software Feature Changes)*.

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
5140HI-CMW710-R6652P05~5140HI-CMW710-R6615P07			
New	None	None	None
Modified	None	None	None
5140HI-CMW710-R6615P06			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R6652P05~R6628P40

None

Operation changes in R6628P35

Changed the default of the port-security m-lag load-sharing-mode command from distributed local to centralized.

For a PoE-capable device, the value for the *max-power* argument in the poe max-power command is changed from the range 1000-3000 to the range 1000-35000, in millwatts.

Operation changes in R6615P07

None

Operation changes in R6615P06

First release

Restrictions and cautions

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.

When you use this version of software, make sure you fully understand the restrictions and cautions described in this section.

Restrictions

Restrictions for VXLAN

Before you configure VXLAN settings, you must execute the **switch-mode 1** command in system view to set the system operating mode to VXLAN.

Restrictions for 10-GE interfaces

To connect a 10-GE interface with a GE transceiver module installed to another interface by using a long optical fiber, you must perform the following tasks on the 10-GE 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.

Restrictions for 802.1X

When you enable 802.1X on a Layer 2 aggregate interface, make sure the 802.1X multicast trigger feature is disabled. To disabled the 802.1X multicast trigger feature, use the **undo dot1x multicast-trigger** command.

Restrictions for dynamic Ethernet service instances

A dynamic Ethernet service instance determines that a packet belongs to the matching VSI if the VLAN ID and source MAC address in the packet match the VLAN ID and MAC address in authorization information for a user.

Restrictions for the drop-unknown command in IGMP-snooping/MLD-snooping view

The **drop-unknown** command is not supported in IGMP-snooping/MLD-snooping view.

Restrictions for the convergence time after a master/subordinate switchover

The Layer 2 traffic convergence time after a master/subordinate switchover exceeds 2 seconds in an EVPN network.

Restrictions for the PSE Device

If a PSE cannot supply power correctly, execute the `poe detection-mode simple` command to enable the simple PD detection mode, and enable non-standard PD detection. To enable non-standard PD detection, execute the `poe legacy enable` command in system view or interface view.

Only PSEs that have a model name ending with character B support PD detection mode configuration. To obtain the model name of a PSE, execute the `display poe pse` command.

Cautions

None

Open problems and workarounds

202403270216

- Symptom: A tunnel cannot forward traffic properly.
- Condition: This symptom occurs if you configure a PBR policy, configure the outgoing interface as a tunnel, delete that tunnel, and then re-create that tunnel.
- Workaround: Execute the **shutdown** and **undo shutdown** commands on the tunnel interface to restore traffic forwarding.

202403180668

- Symptom: An M-LAG system records STP dispute logs, leading to traffic interruption. The symptom occurs because of a logic mistake in processing a specific situation.
- Condition: This symptom occurs if the reliability settings are different between the old and the new software versions when the software is upgraded, especially in STP protocol processing.
- Workaround: During the upgrade process, execute the **undo stp dispute-protection** command to avoid issues caused by version differences.

202311210102

- Symptom: On an M-LAG network, STP convergence might be slow.
- Condition: This symptom occurs if you use the **m-lag standalone enable** command to enable the M-LAG standalone mode and then power-cycle the primary M-LAG member device.
- Workaround: Set the delay that the device must wait before changing to M-LAG standalone mode.

List of resolved problems

Resolved problems in R6652P05

202403040340

- Symptom: Packet loss continues for more than 60 seconds after a master/subordinate switchover is performed on an IRF fabric.
- Condition: This symptom occurs if multicast traffic is transmitted over the RPT path and the output interface of the optimal route is on the master device.

202401291764

- Symptom: An authenticated user is online simultaneously on both M-LAG member devices.
- Condition: This symptom occurs if the following operations are performed on an M-LAG network:
A user first comes online through authentication on a single-homing interface of M-LAG 1.
The user comes online through authentication on a single-homing interface of M-LAG 2 and triggers a migration.

202403060066

- Symptom: BFD flapping occurs.
- Condition: This symptom occurs if the deny-mode ACL rule used to match IPv4 packets configured on VLAN-interface 200 matches BFD packets by mistake, resulting in BFD packet loss and BFD flapping.

202402291384

- Symptom: Tunnel traffic received on a non-aggregate interface matches an ACL configured for an aggregate interface by mistake.
- Condition: This symptom occurs if the ACL configured on an aggregate interface incorrectly matches the specific traffic characteristics. When an extension port is allocated to tunnel traffic, the lowest 8 bits coincide with the SRC TRUNK (source port aggregation) match criterion defined in the aggregate interface ACL.

202402040334

- Symptom: The MAC address is not deleted after a static AC on an interface is deleted.
- Condition: This symptom occurs if 802.1x authentication is performed before the static AC is deleted.

202401090475

- Symptom: The keepalive link flaps due to timeout.
- Condition: This symptom occurs if a large number of ARP packets are sent to the CPU.

202401230378

- Symptom: On an IRF fabric, the number of available ARP resources is incorrect.
- Condition: This symptom occurs if the ARP packets move between the member leaf devices repeatedly.

202311150214

- Symptom: On an M-LAG network, the peer link cannot transmit traffic.
- Condition: This symptom occurs if the following operations are performed on an M-LAG network:
 - a. Enable automatic setup of a VXLAN tunnel between M-LAG member devices.
 - b. Shut down the M-LAG interface on one member device.

202307181156

- Symptom: In an EVPN M-LAG network, the member devices might not advertise BGP routes, and Layer 3 traffic cannot be forwarded.
- Condition: This symptom occurs if BGP EVPN sessions are set up in an EVPN M-LAG network.

202310090404

- Symptom: An OSPF route anomaly occurs.
- Condition: This symptom occurs if you shut down the BFD MAD detection interfaces on IRF devices by shutting down the downlink interface and then the uplink interface.

202307051264

- Symptom: The device does not display logs for adding MAC address entries and displays logs only for deleting MAC address entries.
- Condition: This symptom occurs if you configure port security settings on a port and connect the port to the peer end.

202310240312

- Symptom: On an EVPN DRNI system with a tunnel peer link, the peer-link tunnel goes up slowly or even cannot go up.
- Condition: This symptom might occur if default VXLAN decapsulation is enabled for the IP address of loopback 0 and the IP address is the source IP addresses of non-peer-link VXLAN tunnels.

202310240098

- Symptom: After patch installation and device restart, slow device startup and the EVENT_TIMEOUT log might occur.
- Condition: This symptom might occur if DRNI and monitor link are configured together and the device reboots after installation of a patch with the drnid process included.

202308091835

- Symptom: The xmlcfgd process has exceptions in the next installation of a patch after the patch is loaded, because a subprocess has residues.
- Condition: This symptom might occur if a patch is loaded on the controller connected to the device.

202309260374

- Symptom: The ovsdb-server process occasionally terminates abnormally on the device.
- Condition: This symptom might occur when the controller deploys the configuration to the device.

202308291580

- Symptom: Packet loss occurs during the bulk addition or deletion of M-LAG interfaces on an EVPN M-LAG system.
- Condition: This symptom might occur if singlehoming AC-attached interfaces exist on the EVPN M-LAG system, and bulk addition or deletion of M-LAG interfaces is performed during traffic transmission between remote leaf devices and local ACs.

202309182105

- Symptom: The switch sends 802.1X authentication packets and accounting packets to different RADIUS servers because the state of the port security process is incorrect.
- Condition: This symptom occurs if a master/subordinate switchover is performed on an IRF fabric.

Resolved problems in R6628P47

202310090389

- Symptom: The switch reboots after a QoS policy is applied to an aggregate interface.
- Condition: This symptom occurs if the type protocol-type protocol-type-mask option in an ACL rule contained in the QoS traffic class is type 0806 ffff.

202311300105

- Symptom: A valid user fails Web authentication on an interface.

- Condition: This symptom occurs if the IP address of the remote Web server for Web authentication is the same as a Web authentication-free IP address and the following operations are performed:
 - Enable Web authentication on the interface.
 - Remove the Web authentication-free IP address.
 - Disable Web authentication on the interface.
 - Reenable Web authentication on the interface and reconfigure the Web authentication-free IP address.

202308160716

- Symptom: A user obtains an authorization ACL after it passes authentication and comes online. However, the port ranges in the ACL rules cannot take effect.
- Condition: This symptom occurs if the ACL number is not 2304 and the device is operating in switch mode.

202309121745

- Symptom: On an IRF fabric, multicast forwarding is abnormal after a master/subordinate switchover.
- Condition: This symptom occurs after a master/subordinate switchover if you have configured Layer 3 interfaces before setting up the IRF fabric.

202311141523

- Symptom: In a VXLAN network, all VTEPs have a large number of unnecessary NS/NA packets on the tunnel side. As a result, the CPU usage is high.
- Condition: This symptom occurs if the centralized gateway device is disabling from learning the ND entries on the tunnel side and configured with local ND proxy.

202311180396

- Symptom: The system prompts that VSI resources are insufficient when no VSIs are created.
- Condition: This symptom occurs if you change the link mode of an Ethernet interface to the Layer 3 mode in standard operating mode.

202311150193

- Symptom: The device reboots because of deadlock.
- Condition: This symptom occurs if the **debug qac1 show acl-resc slot 1 chip 0 all** command is executed and the total number of ACLs exceeds 2000.

202309090594

- Symptom: Residual dynamic ACL entries exist on subordinate devices in an IRF fabric.
- Condition: This symptom occurs if the following conditions exist:
 - The IRF fabric has aggregate interfaces that contain member ports from multiple member devices.
 - MAC authentication users are assigned authorization VSIs after they pass MAC authentication and come online.
 - The MAC authentication users are frequently moving among the aggregate interfaces in different VLANs.

202308300886

- Symptom: The device cannot learn ARP entries for endpoints.
- Condition: The symptom might occur when the following conditions exist:
 - Two endpoints access the device from different VLANs and the device acts as the gateway for the two endpoints.

- The two endpoints use only PTP service traffic for communication.
- You execute the **reset arp all** command on the device.

202307130972

- Symptom: After the m-lag extra-vlan command is executed, the M-LAG member devices cannot synchronize ARP or ND entries for the extra VLANs through the peer-link interface.
- Condition: This symptom might occur if some M-LAG interfaces are not assigned to the extra VLANs, and the device is rebooted or the peer-link interface flaps.

202309182105

- Symptom: The switch sends 802.1X authentication packets and accounting packets to different RADIUS servers because the state of the port security process is incorrect.
- Condition: This symptom occurs if a master/subordinate switchover is performed on an IRF fabric.

202305080149

- Symptom: On an EVPN M-LAG network, packet loss occurs when a device single-homed to a leaf device pings other devices.
- Condition: This symptom occurs if a device single-homed to a leaf device broadcasts the received RARP packets on an EVPN+M-LAG network. As a result, ARP entries and ARP suppression entries become incorrect on other devices.

202307271094

- Symptom: The queue priority of common Hello packets is not high enough on an RRPP network.
- Condition: This symptom occurs on an RRPP network.

202306240066

- Symptom: ARP entries are learned on the IPP incorrectly. As a result, remote IP addresses on the same subnet might fail to be accessed.
- Condition: This symptom occurs if proxy ARP is configured for the DRNI dual-active VLAN gateways or VRRP and periodic automatic ARP scanning is enabled by using the **arp scan auto enable** command.

Resolved problems in R6628P43

202308161024

- Symptom: Traffic forwarding fails because ARP entries fail to be learned.
- Condition: This symptom occurs if the configured inbound rate limit is greater than 1 Gbps.

202308160701

- Symptom: Protocol packets that pass through the device are dropped abnormally.
- Condition: This symptom might occur when the rate of protocol packets sent to the CPU is so high that triggers deployment of attack defense ACLs.

202308160698

- Symptom: An aggregate interface flaps and drops packets when the rate of an aggregation member port is edited.
- Condition: This symptom occurs if the rate of an aggregation member port is edited.

202308160692

- Symptom: When the VPN binding limit for Layer 3 aggregate subinterfaces is exceeded, the device does not output any message.
- Condition: This symptom occurs if the VPN binding limit for Layer 3 aggregate subinterfaces is exceeded.

202308160716

- Symptom: A user obtains an authorization ACL after it passes authentication and comes online. However, the port ranges in the ACL rules cannot take effect.
- Condition: This symptom occurs if the ACL number is not 2304 and the device is operating in switch mode.

202308111636

- Symptom: Service failure causes packet forwarding failure.
- Condition: This symptom might occur when the device receives a large number of HTTP or HTTPS attack defense packets destined for the device.

202308101193

- Symptom: A Layer 3 aggregate interface is deleted after VPNs are bound to its subinterfaces, and related ACL resources are not deleted completely.
- Condition: This symptom occurs if a Layer 3 aggregate interface is deleted after VPNs are bound to its subinterfaces.

Resolved problems in R6628P40

202306270487

- Symptom: A packet filter cannot drop the TCP packets with port 639.
- Condition: This symptom occurs when you configure a packet filter to drop TCP packets with port 639.

202305251379

- Symptom: The CPU usage is high on the leaf devices in an EVPN network.
- Condition: This symptom occurs if ARP flood suppression works in response mode and the devices attached to the leaf devices migrate frequently, which causes IP address conflicts.

202305290972

- Symptom: After a service card is restarted or removed, IKE negotiation fails, resulting in interruption of the IPsec service.
- Condition: This symptom occurs if the device has multiple MPUs and a primary/backup switchover occurs.

202306301119

- Symptom: On an RRPP ring, multicast traffic fails to be forwarded after a link switchover is performed.
- Condition: This symptom occurs if you have enabled dropping unknown multicast data packets globally.

202305250569

- Symptom: Residual IPv6SG bindings exist after you clear ND snooping entries in a VLAN.

- Condition: This symptom might occur if you configure the device to create both ND snooping entries and IPv6SG bindings for a VLAN. An endpoint migrates frequently within the VLAN and sends NS packets to the device.

202306130155

- Symptom: After a user goes offline, its IPv6 address binding entries are not deleted.
- Condition: This symptom occurs if ND snooping is configured for a VSI and a large number of endpoints migrate between ACs of the VSI frequently and send ND packets.

202305251218

- Symptom: The device outputs free memory early-warning notifications every hour if you edit the configured free-memory thresholds by adding the early-warning threshold and sufficient-memory threshold after a free-memory alarm has been triggered.
- Condition: This symptom might occur if a free-memory alarm has been triggered without the early-warning threshold and the sufficient-memory threshold configured.

202306301160

- Symptom: After a Layer 3 aggregate interface bound to a VPN instance is deleted, relevant ACL resources remain.
- Condition: This symptom occurs if you bind a Layer 3 aggregate interface to a VPN instance, and then delete the Layer 3 aggregate interface directly.

202305251252

- Symptom: A user fails HWTACACS authorization and accounting.
- Condition: This symptom occurs if the following operations are performed:
 - a. Use the **ip host** or **ipv6 host** command to configure the host name of an HWTACACS server.
 - b. In HWTACACS scheme view, specify the HWTACACS server by its host name and use it as the authentication, authorization, and accounting servers.

202306130886

- Symptom: The SNMP collected traffic statistics is not consistent with the actual statistics.
- Condition: This symptom occurs if the inbound or outbound accumulated traffic statistics on the network management port exceeds 4294967295.

202306150365

- Symptom: The device cannot ping the PCs attached to access ports, and the PCs attached to trunk ports can be pinged.
- Condition: This symptom occurs if ports join an aggregation group, a VPN instance is bound to the related Layer 3 aggregate interface, and ACL configuration is issued to the ports.

202305251257

- Symptom: An M-LAG peer-link interface cannot forward packets of 1859 bytes or larger.
- Condition: This symptom occurs if an M-LAG peer-link interface forwards traffic.

202306250055

- Symptom: A VRRP network cannot be established.
- Condition: This symptom occurs if the intermediate device is not configured with VRRP and is enabled with dropping unknown multicast data packets for a VLAN.

202306250483

- Symptom: You cannot use SSH or Telnet to log in to the local device from another directly connected device.

- Condition: This symptom occurs if the following Web authentication-free subnets exist on the local device:
 - Web authentication-free subnet that contains the IP address for SSH or Telnet login.
 - Web authentication-free subnet that has a mask shorter than the mask of the IP address for SSH or Telnet login.

202306061815

- Symptom: The switch generates a core file for the PIM module.
- Condition: This symptom occurs if the next hop of the optimal route to the source in an SSM multicast forwarding entry is a secondary IP address and route flapping occurs.

202305181213

- Symptom: The switch reboots due to KernelAbnormalReboot.
- Condition: This symptom occurs when multicast settings are configured on an IRF fabric.

202305291037

- Symptom: An ucmd exception occurs when you enter a command.
- Condition: This symptom occurs when HWTACACS command accounting is configured and the server changes from unreachable to reachable.

202306122053

- Symptom: When all online users that are assigned the same authorization ACL go offline, the device fails to delete the authorization ACL information. Residual authorization ACL information exists on the device. As a result, the ACL resources are insufficient.
- Condition: This symptom occurs if the following operations are performed:
 - a. Assign the authorization ACL to multiple BYOD online users in the same VSI.
 - b. Log off all the users. The first online user assigned the authorization ACL is not the last one to go offline.

202305290786

- Symptom: When conversational learning is enabled for forwarding entries of an AC, the device cannot issue AC forwarding entries to the hardware upon receiving traffic on the AC.
- Condition: This symptom occurs if the AC is continuously receiving known unicast packets when you enable conversational learning for forwarding entries of the AC.

202306201965

- Symptom: A MAC authenticated user cannot obtain an IP address after it is assigned to the BYOD authorization VSI.
- Condition: This symptom occurs if the following conditions exist:
 - AD-Campus 6.3 solution.
 - IRF and EVPN VXLAN network.
 - MAC-based traffic match mode is disabled for dynamic Ethernet service instances on the interface on which the user is authenticated. This mode is configured by using the **mac-based ac** command.
 - The user must pass MAC portal authentication on the leaf device, and it has passed MAC authentication.

202305300747

- Symptom: Known unicast traffic is not isolated between VXLAN tunnels of different VXLANs.
- Condition: This symptom occurs if packets are forwarded between two VXLAN tunnel interfaces.

202305251496

- Symptom: The **undo telnet server enable** command cannot take effect.
- Condition: This symptom occurs if you execute this command when the device acts as the Telnet server and the third-party Telnet client does not support option negotiation.

202307010424

- Symptom: If the physical interface on which a PW resides receives more than 500 DHCP Discover messages per second, services (such as OSPF) running on that interface will be interrupted.
- Condition: This symptom occurs if the following conditions exist:
 - a. The device is on the MPLS L2VPN network and is enabled with the DHCP service.
 - b. The PW interface receives more than 500 DHCP Discover messages per second.

202305290977

- Symptom: NAT port blocks for users run out easily, which causes insufficient port blocks and affects user services.
- Condition: This symptom might occur when you configure DNS disabled with ALG in a NAT scenario. Five-tuple entries are generated and the aging timer for the entries is prolonged.

202305290958

- Symptom: A user fails HWTACACS authentication and cannot log in to the Web interface of the device.
- Condition: This symptom occurs if HWTACACS authentication is configured for login and the user attempts to log in to the Web interface of the device.

202305290894

- Symptom: A SmartMC member repeatedly prints the following login failure log after it reboots:
Feb 24 14:41:31:3042023 H3C NETCONF/6/SOAP_XML_LOGIN: admin from 127.0.0.1
loginfailed
- Condition: This symptom occurs if you perform the following operations on the commander:
 - a. Modify the password for the default user (admin) on members.
 - b. Save the member configuration and reboot the command.

202305290914

- Symptom: In a DR system, the outgoing interface for traffic is incorrect after ND entries migrate.
- Condition: This symptom occurs if a DR member device reboots and synchronizes ND entries with the DR peer, ND entries migrate on the DR member device, and the outgoing interface for traffic changes.

202305260074

- Symptom: The output from the **display lldp neighbor-information list** command is displayed in garbled characters when LLDP is enabled on the device.
- Condition: This symptom occurs if LLDP is enabled on the device and you execute **display lldp neighbor-information list** to display brief LLDP information that all LLDP agents received from the neighboring devices in a list.

202305251384

- Symptom: Command execution fails. The CLI gets stuck.
- Condition: This symptom occurs if you execute the **default** command, MAC authentication commands, or port security commands on a port during optimized automated deployment of the AD-Campus 6.3 solution.

202305251188

- Symptom: Some DDNS features are unavailable.
- Condition: This symptom might occur when you send packets to the DDNS server in which the **Host** field is an IP address instead of its corresponding domain name.

202305251147

- Symptom: The IKED process on the MPU experienced an exception, which triggered the device to reboot abnormally.
- Condition: This symptom occurs if IPsec and DPD are deployed, the device acts as the headquarters device, has a large number of IKE packets to handle, and has run for a long time.

202305251580

- Symptom: The output from the **display resource-monitor** command shows that the VSI resource specification is 2K, which does not match the specification list.
- Condition: This symptom occurs if you execute the **display resource-monitor** command to view VSI resource information.

202305130310

- Symptom: The following CAR-exceeded packet loss log is mistakenly reported:
%Apr 18 04:49:15:237 2023 zubojieru-sw DRVPLAT/4/SOFTCAR DROP: -Slot=2;
PktType=UNKNOWN_IPV4MCiptAKNOWN_IPV4MC , SrcMAC=642f-c7aa-d401, Dropped at Stage=0, StageCnt=0, TotalCnt=1.
- Condition: This symptom occurs after the switch receives an unknown multicast packet and creates a drop-unknown entry.

202305200041

- Symptom: The ACL resources are insufficient because the ACL resource occupation mode of voice VLAN is still the port mode after it is configured as the global mode.
- Condition: This symptom occurs if IP phones are automatically discovered through LLDP.

202305230595

- Symptom: A device cannot access the local device by using SSH through an aggregate interface. However, that device can ping the local device.
- Condition: This symptom occurs if the following operations are performed on the local device:
 - a. Configure remote Web authentication.
 - b. Use the **web-auth free-ip** command to specify Web authentication-free subnets.
 - c. Enable Web authentication on the aggregate interface and an Ethernet interface.
 - d. Remove the Web authentication-free subnets.
 - e. Reconfigure the Web authentication-free subnets.

202306070855

- Symptom: Packets carry incorrect source MAC addresses after being forwarded by an EVPN M-LAG system.
- Condition: This symptom might occur if packets received on a tunnel interface are forwarded at Layer 3 over the peer-link to a singlehomed M-LAG interface on the M-LAG peer.

Resolved problems in R6628P35

202303280502

- Symptom: The **display interface brief** command displays a nonexistent management port (MGEO/0/2) when it is executed on an IRF fabric.
- Condition: This symptom might occur when you execute the **display interface brief** command on an IRF fabric.

202303130130

- Symptom: Traffic coming into an AC interface is sent out of that AC interface, forming a loop.
- Condition: This symptom occurs when the AC interface receives traffic whose source MAC address is the same as its destination MAC address.

202303101546

- Symptom: After obtaining an IPv6 address through DHCPv6, the device fails to add the default route to its routing table.
- Condition: This symptom might occur if a device uses DHCPv6 for IPv6 address acquisition.

202303280505

- Symptom: The device cannot communicate with the directly connected peer device through IPv6, and the packet loss ratio approaches 100%.
- Condition: This symptom occurs if a large number of unknown multicast packets exist between the devices and therefore ICMPv6 packets are abnormally dropped.

202303101686

- Symptom: Enable the DHCP snooping entry auto backup feature, and back up the DHCP snooping entries for one time. When you use the **dhcp snooping binding database update now** command to manually save DHCP snooping entries to the backup file again, the backup fails. In this case, the Status field displays writing in the command output from the **display dhcp snooping binding database** command.
- Condition: This symptom occurs if the TFTP server does not support the protocol length feature.

202303031164

- Symptom: After a SmartMC member device restarts, the device keeps reporting log messages for local login failures. The log content is "Feb 24 14:41:31:3042023 H3C NETCONF/6/SOAP_XML_LOGIN: admin from 127.0.0.1 loginfailed."
- Condition: This symptom might occur if you use **smartmc tc password** on the commander to edit the password of default user **admin** for members, save member configurations, and then restart members.

202303101381

- Symptom: The IRF fabric reboots because the memory is exhausted.
- Condition: This symptom occurs if a master/subordinate switchover is performed or a DHCP client requests multiple addresses from the IRF fabric acting as a DHCP relay.

202304101304

- Symptom: An AP attached to an M-LAG system cannot obtain an IP address.
- Condition: This symptom occurs if the M-LAG member devices act as management gateways and ARP snooping is enabled on them.

202303141487

- Symptom: The DHCP process exits unexpectedly and then recovers after DHCP relay entries are aged out.
- Condition: This symptom occurs if the following conditions exist:
 - The switch acts as a DHCP relay.
 - A DHCP client obtains two IP addresses on an interface and then obtained one of the two addresses on another interface.
 - The DHCP relay entries are aged out.

202303240777

- Symptom: When the device is automatically deployed, some ports fail to be assigned to an aggregation group.
- Condition: This symptom occurs if the device is automatically deployed and multiple ports are assigned to the same aggregation group.

202303220706

- Symptom: When the RADIUS authentication server for 802.1X authentication is unreachable, users cannot bypass authentication through the none authentication method.
- Condition: This symptom occurs if the RADIUS authentication server is unreachable and the none authentication method is used.
- Workaround: Execute the **dot1x critical eapol** command.

202303100258

- Symptom: A server attached to an EVPN M-LAG system cannot ping an external network.
- Condition: This symptom might occur if an M-LAG interface with the lacp edge-port setting configured flaps repeatedly.

202302270531

- Symptom: After an IRF fabric splits, the subordinate device cannot detect loops.
- Condition: This symptom might occur if an IRF fabric splits.

202303030899

- Symptom: BGP sessions flap.
- Condition: This symptom might occur if the device receives a large number of packets that do not match any routes.

202302201089

- Symptom: The device does not support collecting packet statistics on Layer 3 aggregate subinterfaces.
- Condition: This symptom might occur if the traffic-statistic enable command is executed on Layer 3 aggregate subinterfaces.

202302170758

- Symptom: Track is associated with EAA. When the state of a track entry changes from negative to positive, the monitoring policy action is not executed.
- Condition: This symptom might occur if a track monitoring event is associated with multiple track entries and one of the track entries changes from not ready state to positive state.

202303090021

- Symptom: On an IRF fabric, traffic received on a Layer 3 aggregate interface cannot be forwarded between the IRF member devices.

- Condition: This symptom might occur if a Layer 3 aggregation group is created before IRF physical interfaces are bound to IRF ports.

202302240358

- Symptom: The device reboots unexpectedly because of a kernel exception.
- Condition: This symptom might occur if the display diagnostic-information command is executed.

202301092178

- Symptom: When a TFTP server is used to save auto backup DHCP snooping entries, only one entry can be stored.
- Condition: This symptom occurs if a TFTP server is used to save auto backup DHCP snooping entries.

202302160003

- Symptom: Static EVPN MAC address entries synchronized from the remote VTEP to the local VTEP are deleted.
- Condition: This symptom occurs if only static EVPN MAC address entries are synchronized from the remote VTEP to the local VTEP. The synchronized EVPN MAC address entries are deleted after an aging period.

202302101133

- Symptom: When a VXLAN tunnel is used as a peer link on an EVPN M-LAG network, the broadcast packets received on the peer link are incorrectly forwarded to the local M-LAG interface.
- Condition: This symptom occurs if broadcast packets are received on the peer link.

202302101493

- Symptom: On an IRF fabric, the SNMP server does not receive link-down alarms from IRF physical interfaces.
- Condition: This symptom occurs if a service interface of the subordinate IRF member device is connected to the SNMP server and the IRF physical interfaces go down.

202212300039

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if MQC configuration matches both IPv4/IPv6 packets and packets with multiple outer VLAN tags.

202302021438

- Symptom: The switch prints an error message when a DHCPv6 client requests an IPv6 prefix from the DHCPv6 server through the switch.
- Condition: This symptom occurs if the switch acts as a DHCP snooping device and you have executed the **ipv6 dhcp snooping pd binding record** and **ipv6 verify source ip-address mac-address** commands on the switch.

202301110093

- Symptom: On an M-LAG system, ARP entries and MAC address entries are incorrect, and the peer link cannot be used to forward traffic.
- Condition: This symptom occurs if the M-LAG system is automatically deployed by using devices that start up with initial configuration.

202301111261

- Symptom: On an EVPN VXLAN M-LAG system formed by two leaf devices, reboot of one M-LAG member device results in reboot of the other M-LAG member device. The M-LAG system resumes operation after multiple automatic reboots.
- Condition: This symptom occurs if 1500 MAC authentication users access the network through ARP learning and the primary member device is rebooted.

202212300039

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if MQC configuration matches both IPv4/IPv6 packets and packets with multiple outer VLAN tags.

202301060304

- Symptom: A delay exists when MAC authentication users access the network.
- Condition: This symptom occurs if MAC authentication users go offline after successful authentication and MAC authentication is triggered again.

202212081055

- Symptom: The device cannot come online because the **ipv6 address dhcp-alloc** command on VLAN interface 1 is lost.
- Condition: This symptom occurs if the automatic configuration process ends or you manually terminate the automatic configuration process during an IPv6 automatic deployment.

202212080022

- Symptom: The device reboots when a large number of MAC authentication users come online and go offline on an aggregate interface and ACLs and URLs are authorized to the users.
- Condition: This symptom occurs might if a large number of MAC authentication users come online and go offline on an aggregate interface and ACLs and URLs are authorized to the users.

202208301357

- Symptom: An endpoint cannot pass Web authentication in an M-LAG system.
- Condition: This symptom occurs if the following conditions exist:
 - The distributed even-/odd-MAC mode is configured for authentication load sharing.
 - The MAC address of the endpoint is an odd MAC address.
 - The authentication packets are sent to the M-LAG member device in distributed even-MAC mode.

202211280698

- Symptom: When a route server reflects an EBGP route, it mistakenly modifies the router MAC address in the route as its own router MAC address.
- Condition: This symptom occurs if you have executed both the **peer route-server-client** and **peer router-mac-local dci** commands on the route server.

202211240773

- Symptom: A clients reports two different XPATH messages, and another client reports no messages.
- Condition: This symptom occurs if you configure gNMI subscriptions and concurrent sessions exist.

202301040134

- Symptom: An error occurs during device startup.
- Condition: This symptom occurs if the device starts up.

202301040841

- Symptom: After you execute the **display mad verbose** command on an IRF member device, the command output displays both VLAN interfaces and excluded ports while only VLAN interfaces should be displayed.
- Condition: This symptom occurs if an IRF fabric is split and then established.

202207050531

- Symptom: After you delete an interface, the resources allocated to the interface cannot be released. As a result, the system cannot allocate these resources to other functions.
- Condition: This symptom occurs if you delete the source interface specified for VXLAN default decapsulation.

202212280017

- Symptom: In an EVPN multicast network, the multicast traffic is mistakenly forwarded.
- Condition: This symptom occurs if the device forwards multicast traffic.

202212280016

- Symptom: A QoS policy on an M-LAG member device fails to match with the packets sent from the peer.
- Condition: This symptom occurs if an M-LAG member device configured with a QoS policy receives packets from the peer through the peer link in an M-LAG system.

202301051651

- Symptom: Failed to restore the default settings for a SmartRate-Ethernet interface by executing the **default** command.
- Condition: This symptom occurs if you have executed the **stp instance 0 port priority 16** command on a SmartRate-Ethernet interface.

202301040139

- Symptom: In an M-LAG system, the interfaces in M-LAG MAD DOWN state fail to restore to normal after an M-LAG member device restarts.
- Condition: This symptom occurs if the member port rates of the peer link interface are inconsistent.

202212220265

- Symptom: The device fails to issue the **m-lag extra-vlan** command through NETCONF for the first time.
- Condition: This symptom occurs if the device issues the **m-lag extra-vlan** command through NETCONF for the first time after device startup.

202212281015

- Symptom: In a VXLAN network configured with M-LAG, the device acting as a leaf node drops multicast packets from the spine.
- Condition: This symptom occurs when the leaf node receives multicast packets from the spine in a VXLAN network configured with M-LAG.

202212260304

- Symptom: The OSPF neighbors and PIM neighbors flap.
- Condition: This symptom occurs if the device receives a large number of multicast packets with TTL 1.

202212191223

- Symptom: On an MPLS network, the VSI TTI configuration is not cleared after you configure AC settings and then restore the device to empty configuration.
- Condition: This symptom occurs if you configure AC on the device and then restore the empty configuration for the device.

202212060168

- Symptom: No output is displayed upon execution of the **display kernel reboot** command.
- Condition: This symptom might occur when you execute the **display kernel reboot** command to view information about device reboot events.

202211181050

- Symptom: In an M-LAG network, online 802.1X user go offline and new users cannot come online after one member device (leaf device) is upgraded.
- Condition: This symptom occurs if you form an M-LAG network by using two leaf devices and upgrade one leaf device

202207111528

- Symptom: No commands can be entered after the **dmesg** command is executed.
- Condition: This symptom occurs if you enter the **dmesg** command in kdb view after the device is power cycled.

202208051014

- Symptom: In a VPLS network, the packets of a PW have inner encapsulation errors.
- Condition: This symptom occurs if you flap the PW-side interface repeatedly.

202208040950

- Symptom: VPLS packets fail to be forwarded in an MPLS network with P devices.
- Condition: This symptom occurs if the outgoing label on the public network PE is the same as the incoming label on the P device.

202207220046

- Symptom: Endpoints fail to be obtain IP addresses from the IRF fabric acting as a DHCP server.
- Condition: This symptom occurs if the IRF fabric connects to the AC interface and experiences a master/subordinate switchover.

202206020061

- Symptom: Cross-subnet packets cannot be forwarded in hardware.
- Condition: This symptom occurs if the peer device is enabled with source MAC check.

202208041205

- Symptom: The HardwareRev information about a subcard read through NETCONF is wrong.
- Condition: This symptom occurs if you read the HardwareRev information about a subcard through NETCONF.

202206161204

- Symptom: A user fails to obtain an IP address and fails to come online after the user.
- Condition: This symptom occurs if the following conditions exist:
 - Policy check is enabled on the server.
 - The user comes online from the isolation security group and passes security checks.
 - The user is switched to the service security group.

202206210576

- Symptom: The configuration fails to take effect because the free memory is insufficient.
- Condition: This symptom occurs if a physical interface goes down and comes up frequently.

202206250439

- Symptom: The VPN instance associated with interface does not take effect after the device reboots
- Condition: This symptom occurs if you associate the same VPN instance with a Layer 3 Ethernet subinterface and a VLAN interface that have the same interface number.

202205231332

- Symptom: PoE current is not displayed in the output from the display poe-power command.
- Condition: This symptom might occur if the following conditions exist:
 - A GRE power supply and an LITEON power supply are installed on the device.
 - The GRE power supply supplies power and the LITEON power supply does not supply power

202112271474

- Symptom: Member devices in a VXLAN DR system might reboot unexpectedly.
- Condition: This symptom might occur if a certain script is executed.

202109060975

- Symptom: PIM DM is disabled on a VLAN interface, Layer 2 multicast entries are not established on the subordinate IRF member device, and multicast traffic is broadcast within the VLAN.
- Condition: This symptom occurs if both Layer 2 multicast and Layer 3 multicast are configured for the same VLAN, traffic is received on the subordinate IRF member device, and IGMP snooping is configured for the VLAN on an IRF fabric.

202205270372

- Symptom: Outgoing packets carry an incorrect source MAC address.
- Condition: This symptom occurs if the following operations have been performed:
 - Configure a MAC address on a VLAN interface.
 - Delete the VLAN interface and re-create it.

202205240571

- Symptom: Threads of OSPFv3 access invalid pointers and are hanged, the core is abnormal, and routes are not updated.
- Condition: This symptom occurs if the following operations are performed:
 - a. Configure a VPN instance that has no OSPFv3 instances.
 - b. Associate the VPN instance with an interface and execute the **ipv6 address** command on the interface.
 - c. Execute OSPFv3 preconfigured commands but not OSPFv3 enable commands. The **ospfv3 1 area 0 command** is an example of OSPFv3 enable commands. OSPFv3 preconfigured commands refer to commands other than enable commands, such as **ospfv3 timer hello**, **ospfv3 network-type**, and **ospfv3 cost**.
 - d. Remove the VPN instance-interface association or delete the VPN instance.

202204110848

- Symptom: Source ports in a local mirroring group fail to be configured after the source ports in another local mirroring group are configured.

- Condition: This symptom occurs if the following operations are performed:
 - Configure the monitor port as the same port for seven local mirroring groups.
 - Configure the source ports for the seventh local mirroring group.
 - Configure the source ports for another local mirroring group among the remaining local mirroring groups.

202110261296

- Symptom: In an inter-VPN forwarding scenario, multicast traffic cannot be forwarded to the public network.
- Condition: This symptom occurs if a member port is repeatedly added to and removed from the aggregate interface for the tunnel and the private route flaps.

202112310599

- Symptom: The device issues Layer 3 IPv4 multicast entries successfully and might fail to issue some Layer 3 IPv6 multicast entries, which causes multicast forwarding errors.
- Condition: This symptom might occur if the device issues 3000 IPv4 IPMC multicast entries and then 250 IPv6 IPMC multicast entries and the number of multicast entries reaches the upper limit.

Resolved problems in R6615P07

202205111296

- Symptom: A VSI interface in down state can still act as a gateway interface to forward traffic.
- Condition: This symptom occurs if the **shutdown** command is executed on a VSI interface configured as the VXLAN gateway interface.

202205111299

- Symptom: When a PoE interface fails to supply power, the traps cannot correctly report the failure.
- Condition: This symptom occurs if the maximum power configured on the PoE interface cannot meet the power requirements of the attached PDs.

202205111292

- Symptom: Within 5 minutes after the VCF fabric is automatically deployed, the devices try to obtain the device list file.
- Condition: This symptom occurs if legacy automated deployment is performed for the devices and the device list is not configured.

202205111301

- Symptom: After the VCF fabric is automatically deployed, the original PVID settings of interfaces are lost.
- Condition: This symptom occurs if a device is automatically deployed as an access device, the interfaces have original PVID settings, the interfaces are connected to APs, and then the APs are removed.

202203300334

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if an AC is associated with a VSI on the device.

202201200603

- Symptom: When loop detection is configured on a VSI and ARP packets are injected to a blocked AC, the AC can still respond with ARP replies normally.

- Condition: This symptom occurs if ARP proxy is configured on the VSI.

202108170529

- Symptom: The MAC address entries for MAC authentication users and 802.1x users are not deleted after they go offline.
- Condition: This symptom occurs if MAC authentication users and 802.1x users move between member devices on an IRF fabric.

202203211300

- Symptom: After a transceiver module is installed into a port, the device reboots unexpectedly.
- Condition: This symptom occurs if the following conditions exist:
 - a. A DR system has peer links.
 - b. Configure an AC on the DR interface (an aggregate interface).
 - c. On a single-homed interface, configure an AC with the same service instance.

202201050390

- Symptom: A MAC address entry does not age out if the MAC address moves between two interfaces constantly.
- Condition: This symptom might occur if two interfaces receive packets sourced from the same MAC address.

202112281596

- Symptom: An EVPN DR system uses an Ethernet aggregate link as the IPL. After an AC is deleted and recreated, the AC does not take effect.
- Condition: This symptom might occur if the following events occur:
 - a. The maximum number of ACs is reached.
 - b. A static AC is deleted and recreated on a non-DR interface or DR interface.

202112280428

- Symptom: MAC address entries are not deleted completely, and the type of the MAC address entries is incorrect.
- Condition: This symptom might occur if the following events occur on a DR system formed by two devices with different capabilities:
 - a. The traffic load reaches the limit of the device with higher capabilities.
 - b. The reset l2vpn mac command is executed.

202112270862

- Symptom: An EVPN DR system does not forward the broadcast traffic received from DR interfaces over the IPL.
- Condition: This symptom might occur if the configuration is rolled back after the `b_evpn_drni_no_peer_link_1_3_3.tc` script is executed.

202112301425

- Symptom: On an EVPN DR system, synchronized MAC addresses are issued to incorrect ACs, and this issue cannot be recovered.
- Condition: This symptom might occur if ACs match single-tagged packets and the following operations are performed:
 - a. ACs matching the same VLAN are mapped to different VSIs.
 - b. The ACs are deleted.
 - c. The ACs are recreated to match the same VLAN and mapped to the same VSI.

202201040231

- Symptom: The device fails to forward some multiple packets.
- Condition: This symptom might occur if BIDIR-PIM is enabled and RPs are configured in BIDIR-PIM domains.

202112280864

- Symptom: MAC address learning is disabled globally when the device is receiving dense traffic, but dynamic MAC address entries are not deleted.
- Condition: This symptom might occur if MAC address learning is disabled globally when the device is receiving dense traffic.

202111260029

- Symptom: MAC address entries created for MAC authentication users are not deleted after MAC authentication is disabled on DR interfaces.
- Condition: This symptom might occur if MAC authentication is disabled on DR interfaces of a DR system that uses an Ethernet aggregate link as the IPL.

202110191417

- Symptom: Once removed from a monitoring group, an interface cannot be assigned to monitoring groups again.
- Condition: This symptom might occur if traffic is mirrored to a monitoring group through local mirroring and flow mirroring.

202112081609

- Symptom: On an EVPN DR system, a BGP task is abnormal and creates a core file.
- Condition: This symptom might occur if the DR system receives ARP packets and 1000 attached hosts migrate from the DR system.

202112291428

- Symptom: A non-existent VLAN is created on the primary DR device in type 2 configuration consistency check.
- Condition: This symptom might occur if the following operations are performed:
 - a. Two devices are booted with initial configuration, and they are configured to set up a DR system.
 - b. The keepalive link comes up.
 - c. An IPP is configured on the primary and secondary devices in sequence.

202112291070

- Symptom: Users fail authentication after the attached IRF fabric reboots.
- Condition: This symptom might occur if an IRF master/subordinate switchover occurs when the interface used for authentication is down and users are online.

202112250446/202112081895

- Symptom: EVPN and Layer 2 multicast are configured on the device, and the **igmp-snooping drop-unknown** setting does not take effect.
- Condition: This symptom might occur if a VXLAN ID is deleted and recreated on a VSI.

202112081745

- Symptom: The device generates blackhole MAC address entries and does not forward certain traffic.
- Condition: This symptom might occur if incoming traffic matches a MAC-based VLAN and an IP subnet-based VLAN simultaneously on the same interface.

202112271474

- Symptom: Member devices in a VXLAN DR system might reboot unexpectedly.
- Condition: This symptom might occur if a certain script is executed.

202110210626

- Symptom: AC resources for a VSI might not be deleted completely when an authentication user logs off and then logs on again.
- Condition: This symptom might occur if user MAC addresses move between interfaces and a large number of authentication users exist.

202112131788

- Symptom: EVPN is enabled to forward Layer 2 multicast traffic. After a VXLAN ID is deleted and then created again, the drop-unknown setting does not take effect.
- Condition: This symptom might occur if a VXLAN ID is deleted and created again with the drop-unknown setting being intact.

202203181089

- Symptom: When all types of MACsec debugging are enabled by using the debugging macsec all command, the system outputs an error message to indicate that it has received an oversized packet. However, the system does not receive an oversized packet.
- Condition: This symptom occurs if MACsec is enabled on a port of the LSWM2XMGT2PM subcard and the local and peer MACsec-enabled ports forward traffic at wire speed.

202203211300

- Symptom: A DR member device reboots unexpectedly after a transceiver module is installed.
- Condition: This symptom might occur if the following conditions exist:
 - a. The DR member devices have a physical IPL between them.
 - b. An Ethernet service instance is configured both on a DR interface and an interface attached to a single-homed device.

Resolved problems in R6615P06

First release

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

Information to collect:

- Technical support registration number (if applicable).
- Product name, model or version, and serial number.
- Operating system name and version.
- Firmware version.

- Error messages.
- Product-specific reports and logs.
- Add-on products or components.
- Third-party products or components.

Documents

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

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

Related documents

The following documents provide related information:

- HPE PSR150-A & PSR150-D Series Power Supplies User Guide
- HPE PSR720-56A Power Supply User Guide
- HPE PSR1110-56A Power Supply User Guide
- HPE X721 Power to Port Fan Tray (5060-0175) & HPE X722 Port to Power Fan Tray (5060-0174) User Guide
- HPE LSWM2XGT2PM Interface Card (JH156A) User Guide
- HPE LSWM2SP2PM Interface Card (JH157A) User Guide
- HPE LSWM2XMGT2PM Interface Card (R9L65A) User Guide
- HPE FlexNetwork 5140 HI Switch Series Installation Guide
- HPE FlexNetwork 5140 HI Switch Series Configuration Guides Index-R66xx
- About the HPE FlexNetwork 5140 HI Switch Series Configuration Guides-R66xx
- HPE FlexNetwork 5520 H Switch Series Fundamentals Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Virtual Technologies Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 2 - LAN Switching Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 3 - IP Services Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 3 - IP Routing Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series IP Multicast Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series MCE Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series ACL and QoS Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Security Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series High Availability Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Network Management and Monitoring Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series Telemetry Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series OpenFlow Configuration Guide-R66xx
- HPE FlexNetwork 5140 HI Switch Series VXLAN Configuration Guide-R66xx

- HPE FlexNetwork 5140 HI Switch Series EVPN Configuration Guide-R66xx
- About the HPE FlexNetwork 5140 HI Switch Series Command References-R66xx
- HPE FlexNetwork 5140 HI Switch Series Fundamentals Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Virtual Technologies Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 2 - LAN Switching Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 3 - IP Services Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Layer 3 - IP Routing Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series IP Multicast Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series MCE Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series ACL and QoS Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Security Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series High Availability Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Network Management and Monitoring Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series OpenFlow Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series Telemetry Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series VXLAN Command Reference-R66xx
- HPE FlexNetwork 5140 HI Switch Series EVPN Command Reference-R66xx
-

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Appendix A Feature list

Hardware features

Table 5 5140HI series hardware features for non-PoE switch models

Item	HPE 5140 24G 4SFP+ 1-slot HI Sw	HPE 5140 48G 4SFP+ 1-slot HI Sw
Dimensions (H × W × D)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)	
Weight	≤ 7 kg (15.43 lb)	
Console ports	1 × Micro USB console port 1 × serial console port Only the Micro USB console port is available when you connect both ports.	
USB port	1	
Management Ethernet port	1	
SFP+ port	4	
SFP port	8	-
10/100/1000 Base-T Ethernet ports	24	48
SFP+ ports	4	
Expansion slot	1, on the rear panel	
Power module slot	2, on the rear panel	
Fan tray slot	2, on the rear panel	
Input voltage	- AC power source - Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz - Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz - DC power source: -48 V DC power source in the equipment room or RPS (recommended HP RPS models: A-RPS800 or A-RPS1600) - Rated voltage: -48 VDC to -60 VDC - Max voltage: -36 VDC to -72 VDC	
Minimum power consumption	- Single AC input: 24 W - Single DC input: 24W - Dual AC inputs: 29 W - Dual DC inputs: 298W	- Single AC input: 27 W - Single DC input: 24W - Dual AC inputs: 31 W - Dual DC inputs: 29 W
Maximum power consumption	- Single AC input: 87W - Single DC input: 88W - Dual AC inputs: 91 W - Dual DC inputs: 95W	- Single AC input: 88W - Single DC input: 89W - Dual AC inputs: 93 W - Dual DC inputs: 96 W

Item	HPE 5140 24G 4SFP+ 1-slot HI Sw	HPE 5140 48G 4SFP+ 1-slot HI Sw
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	
Melting current of power supply fuse	• AC-input: 5 A/250 V • DC-input: 8 A/250 V	
Operating temperature	-5°C to 45°C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	

Table 6 5140HI series hardware features for PoE switch models

Item	HPE 5140 24G PoE+ 4SFP+ 1-slot HI Sw	HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw
Dimensions (H × W × D)	43.6 × 440 × 460 mm(1.72 × 17.32 × 18.11 in)	
Weight	≤ 9.6 kg (21.16 lb)	
Console ports	• 1 × Micro USB console port • 1 × serial console port Only the Micro USB console port is available when you connect both ports.	
USB port	1	
Management Ethernet port	1	
SFP+ port	4	
10/100/1000Base-T Ethernet ports	24	48
Expansion slot	1, on the rear panel	
Power module slot	2, on the rear panel	
Fan tray slot	2, on the rear panel	
Input voltage	• AC input for the PSR360-56A/PSR720-56A power module: ◦ Rated voltage range: 100 VAC to 240 VAC @ 50 Hz or 60 Hz ◦ Max voltage range: 90 VAC to 264 VAC @ 47 Hz to 63 Hz • AC input for the PSR1110-56A power module: ◦ Rated voltage range: 115 VAC to 240 VAC @ 50 Hz or 60 Hz ◦ Max voltage range: 102.5 VAC to 264 VAC @ 47 Hz to 63 Hz You can use a –48 VDC power source in the equipment room or an H3C RPS (RPS1600-A).	

PoE power capacity	Depends on the power module configurations. For more information, see Table 7 .	
Minimum power consumption	31.03W	33.09W
Maximum power consumption (including PoE power consumption)	927.2W	1729W
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	
Melting current of power supply fuse	15 A/250 V	
Operating temperature	-5°C to 45°C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	

Table 7 PoE power capacity of the HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw Swch switches

Power module configuration	HPE 5140 24G PoE+ 4SFP+ 1-slot HI Sw		HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw	
	Total PoE power capacity	Max PoE power capacity per port	Total PoE power capacity	Max PoE power capacity per port
2 × PSR1110-56A	810W	30W	1680w	30 W
1 × PSR1110-56A and 1 × PSR720-56A	810W	30W	1560 W	30 W
1 × PSR1110-56A and 1 × PSR360-56A	810W	30W	1200W	30W
2 × PSR720-56A	810W	30W	1200W	30W
1 × PSR1110-56A	810W	30W	810 W	30 W
1 × PSR720-56A and 1 × PSR360-56A	810W	30W	810 W	30 W
1 × PSR720-56A	450W	30W	450 W	30 W
2 × PSR360-56A	450W	30W	450 W	30 W
1 × PSR360-56A	180W	30W	180 W	30 W

Software features

Table 8 Software features of the 5140HI series

Feature	HPE 5140 24G 4SFP+ 1-slot HI Sw HPE 5140 48G 4SFP+ 1-slot HI Sw HPE 5140 24G PoE+ 4SFP+ 1-slot HI Sw HPE 5140 48G PoE+ 4SFP+ 1-slot HI Sw
Full duplex Wire speed L2 switching capacity	- Excluding subcards: 176 Gbps - Including subcards: - For frames (length=64 bytes): 240 Gbps - For frames (length≥128 bytes): 336 Gbps
Whole system Wire speed L2 switching Packet forwarding rate	180Mpps
Link aggregation	- Aggregation of GE ports - Aggregation of 10-GE ports - Aggregation of 40-GE ports - Static link aggregation - Dynamic link aggregation - Inter-device aggregation - A maximum of 128 inter-device aggregation groups - A maximum of 32 ports for each aggregation group
Flow control	IEEE 802.3x flow control
Jumbo Frame	Supports maximum frame size of 10000
MAC address table	64K MAC addresses 1K static MAC addresses - Blackhole MAC addresses - MAC address learning limit on a port
VLAN	- A maximum of 4094 port-based VLANs - QinQ, selective QinQ, VLAN mapping - Voice VLANs - Protocol-based VLANs - MAC-based VLANs
ARP	- A maximum of 32K ARP entries (a maximum number of 32K ARP entries in later versions) - A maximum of 2K static ARP entries - Gratuitous ARP - ARP attack detection based on DHCP snooping entries, 802.1X entries, and static IPSG bindings - ARP rate limit
ND	16K entries 2K static entries - ND Snooping
VLAN virtual	1K

interface	
DHCP	• DHCP client • DHCP snooping • DHCP relay • DHCP server • DHCP Option82
DHCPv6	• DHCPv6 server • DHCPv6 relay • DHCPv6 client • DHCPv6 snooping
DNS	• Static DNS • Dynamic DNS • IPv4 and IPv6 DNS
unicast route	• IPv4 and IPv6 static routes • RIP/RIPng • OSPF/OSPFv3 • BGP/IPv6 BGP • ISIS/ISISv6
Multicast	• IGMP Snooping • MLD Snooping • multicast VLAN • PIM SM • PIM DM • MSDP
Broadcast/multi cast/unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Bps-based storm control
MSTP	• STP/RSTP/MSTP protocol • 64 Spanning Tree instances • STP Root Guard • BPDU Guard
SmartLink	• 32
RRPP	• RRPP
QoS/ACL	• Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4) • Eight output queues for each port • SP/WRR/SP+WRR queue scheduling algorithms • WRED • Port-based rate limiting • Flow-based redirection • Time range
Mirroring	• Local port mirroring • A maximum number of 7 mirroring groups • Layer 2 remote port mirroring • Flow mirroring
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS

	• SSH 2.0 • Port isolation • 802.1X • Port security • MAC-address-based authentication • IP Source Guard • HTTPS • PKI • EAD
802.1X	• Up to 2K users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • Dynamic 802.1X-based ACL/VLAN assignment
Open Flow	• 16 Instances • 1500 flow entries (issued by using ACL)
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • Remote Monitoring(RMON) • IMC NMS • Web network management (later version) • System log • Hierarchical alarms • IRF • NTP • Power supply alarm function • Fan and temperature alarms
Maintenance	• Debugging information output • Ping and Tracert • Remote maintenance through Telnet • NQA • 802.1ag • 802.3ah • DLDP • Virtual Cable Test

Appendix B Fixed security vulnerabilities

Fixed security vulnerabilities in R6652P05

CVE-2023-2650

Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is $O(n^2)$ with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERS in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERS may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low.CVE-2022-32221

When doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT_READFUNCTION`) to ask for data to send, even when the `CURLOPT_POSTFIELDS` option has been set, if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the subsequent `POST` request. The problem exists in the logic for a reused handle when it is changed from a PUT to a POST.

CVE-2023-2953

A vulnerability was found in openldap. This security flaw causes a null pointer dereference in `ber_memalloc_x()` function.

CVE-2023-0465

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function.

CVE-2023-24329

An issue in the `urllib.parse` component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.

CVE-2023-0286

There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an `ASN1_STRING` but the public structure definition for `GENERAL_NAME` incorrectly specified the type of the `x400Address` field as `ASN1_TYPE`. This field is subsequently interpreted by the OpenSSL function `GENERAL_NAME_cmp` as an `ASN1_TYPE` rather than an `ASN1_STRING`. When CRL checking is enabled (i.e. the application sets the `X509_V_FLAG_CRL_CHECK` flag), this vulnerability may allow an attacker to pass arbitrary pointers to a `memcmp` call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

CVE-2023-0464

A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function.

CVE-2023-0215

The public API function `BIO_new_NDEF` is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new `BIO_f_asn1` filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call `BIO_pop()` on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function `B64_write_ASN1()` which may cause `BIO_new_NDEF()` to be called and will subsequently call `BIO_pop()` on the BIO. This internal function is in turn called by the public API functions `PEM_write_bio_ASN1_stream`, `PEM_write_bio_CMS_stream`, `PEM_write_bio_PKCS7_stream`, `SMIME_write_ASN1`, `SMIME_write_CMS` and `SMIME_write_PKCS7`. Other public API functions that may be impacted by this include `i2d_ASN1_bio_stream`, `BIO_new_CMS`, `BIO_new_PKCS7`, `i2d_CMS_bio_stream` and `i2d_PKCS7_bio_stream`. The OpenSSL `cms` and `smime` command line applications are similarly affected.

CVE-2022-4304

A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

CVE-2023-28321

An improper certificate validation vulnerability exists in curl <v8.1.0 in the way it supports matching of wildcard patterns when listed as "Subject Alternative Name" in TLS server certificates. curl can be built to use its own name matching function for TLS rather than one provided by a TLS library. This private wildcard matching function would match IDN (International Domain Name) hosts incorrectly and could as a result accept patterns that otherwise should mismatch. IDN hostnames are converted to puny code before used for certificate checks. Puny coded names always start with `xn--` and should not be allowed to pattern match, but the wildcard check in curl could still check for `x\*`, which would match even though the IDN name most likely contained nothing even resembling an `x`.

CVE-2023-28322

An information disclosure vulnerability exists in curl <v8.1.0 when doing HTTP(S) transfers, libcurl might erroneously use the read callback (`CURLOPT\_READFUNCTION`) to ask for data to send, even when the `CURLOPT\_POSTFIELDS` option has been set, if the same handle previously was used to issue a `PUT` request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the second transfer. The problem exists in the logic for a reused handle when it is (expected to be) changed from a PUT to a POST. A vulnerability was found in curl.

CVE-2021-3753

A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds read in vt as the write access to vc_mode is not protected by lock-in vt_ioctl (KDSETMDE). The highest threat from this vulnerability is to data confidentiality.

CVE-2021-3739

A NULL pointer dereference flaw was found in the btrfs_rm_device function in fs/btrfs/volumes.c in the Linux Kernel, where triggering the bug requires 'CAP_SYS_ADMIN'. This flaw allows a local attacker to crash the system or leak kernel internal information. The highest threat from this vulnerability is to system availability.

CVE-2021-45868

In the Linux kernel before 5.15.3, fs/quota/quota_tree.c does not validate the block number in the quota tree (on disk). This can, for example, lead to a kernel/locking/rwsem.c use-after-free if there is a corrupted quota file.

CVE-2022-1011

A flaw use after free in the Linux kernel FUSE filesystem was found in the way user triggers write(). A local user could use this flaw to get some unauthorized access to some data from the FUSE filesystem and as result potentially privilege escalation too.

CVE-2022-0854

A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space.

CVE-2022-0492

A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.

CVE-2021-4002

A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data.

CVE-2022-25375

An issue was discovered in drivers/usb/gadget/function/rndis.c in the Linux kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory.

CVE-2020-7469

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

CVE-2021-22924

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

CVE-2021-3753

A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds read in vt as the write access to vc_mode is not protected by lock-in vt_ioctl (KDSETMDE). The highest threat from this vulnerability is to data confidentiality.

CVE-2021-3739

A NULL pointer dereference flaw was found in the btrfs_rm_device function in fs/btrfs/volumes.c in the Linux Kernel, where triggering the bug requires 'CAP_SYS_ADMIN'. This flaw allows a local attacker to crash the system or leak kernel internal information. The highest threat from this vulnerability is to system availability.

CVE-2021-45868

In the Linux kernel before 5.15.3, fs/quota/quota_tree.c does not validate the block number in the quota tree (on disk). This can, for example, lead to a kernel/locking/rwsem.c use-after-free if there is a corrupted quota file.

CVE-2022-1011

A flaw use after free in the Linux kernel FUSE filesystem was found in the way user triggers write(). A local user could use this flaw to get some unauthorized access to some data from the FUSE filesystem and as result potentially privilege escalation too.

CVE-2022-0854

A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space.

CVE-2022-0492

A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.

CVE-2021-4002

A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data.

CVE-2022-25375

An issue was discovered in drivers/usb/gadget/function/rndis.c in the Linux kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory.

CVE-2020-7469

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

CVE-2020-25577

In FreeBSD 12.2-STABLE before r368250, 11.4-STABLE before r368253, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 rtsold(8) does not verify that the RDNSS option does not extend past the end of the received packet before processing its contents. While the kernel currently ignores such malformed packets, it passes them to userspace programs. Any programs expecting the kernel to do validation may be vulnerable to an overflow.

CVE-2020-8284

A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port and this way potentially make curl extract information about services that are otherwise private and not disclosed for example doing port scanning and service banner extractions.

CVE-2020-8285

Curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.

CVE-2021-22924

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

CVE-2021-22925

curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl. This rarely used option is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending `NEW_ENV` variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol. This could happen because curl did not call and use `sscanf()` correctly when parsing the string provided by the application.

CVE-2022-39028

Telnetd in GNU Inetutils through 2.3, MIT krb5-appl through 1.0.3, and derivative works has a NULL pointer dereference via 0xff 0xf7 or 0xff 0xf8. In a typical installation, the telnetd application would crash but the telnet service would remain available through inetd. However, if the telnetd application has many crashes within a short time interval, the telnet service would become unavailable after inetd logs a "telnet/tcp server failing (looping), service terminated" error. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.

CVE-2021-29629

In FreeBSD 13.0-STABLE before n245765-bec0d2c9c841, 12.2-STABLE before r369859, 11.4-STABLE before r369866, 13.0-RELEASE before p1, 12.2-RELEASE before p7, and

11.4-RELEASE before p10, missing message validation in libradius(3) could allow malicious clients or servers to trigger denial of service in vulnerable servers or clients respectively.

CVE-2021-29628

In FreeBSD 13.0-STABLE before n245764-876ffe28796c, 12.2-STABLE before r369857, 13.0-RELEASE before p1, and 12.2-RELEASE before p7, a system call triggering a fault could cause SMAP protections to be disabled for the duration of the system call. This weakness could be combined with other kernel bugs to craft an exploit.

CVE-2021-29626

In FreeBSD 13.0-STABLE before n245117, 12.2-STABLE before r369551, 11.4-STABLE before r369559, 13.0-RC5 before p1, 12.2-RELEASE before p6, and 11.4-RELEASE before p9, copy-on-write logic failed to invalidate shared memory page mappings between multiple processes allowing an unprivileged process to maintain a mapping after it is freed, allowing the process to read private data belonging to other processes or the kernel. 5.5 MEDIUM

CVE-2021-29627

In FreeBSD 13.0-STABLE before n245050, 12.2-STABLE before r369525, 13.0-RC4 before p0, and 12.2-RELEASE before p6, listening socket accept filters implementing the accf_create callback incorrectly freed a process supplied argument string. Additional operations on the socket can lead to a double free or use after free.

CVE-2020-25584

In FreeBSD 13.0-STABLE before n245118, 12.2-STABLE before r369552, 11.4-STABLE before r369560, 13.0-RC5 before p1, 12.2-RELEASE before p6, and 11.4-RELEASE before p9, a superuser inside a FreeBSD jail configured with the non-default allow.mount permission could cause a race condition between the lookup of "." and remounting a filesystem, allowing access to filesystem hierarchy outside of the jail.

In FreeBSD 12.2-STABLE before r368250, 11.4-STABLE before r368253, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 when processing a DNSSL option, rtsold(8) decodes domain name labels per an encoding specified in RFC 1035 in which the first octet of each label contains the label's length. rtsold(8) did not validate label lengths correctly and could overflow the destination buffer.

CVE-2020-7464

In FreeBSD 12.2-STABLE before r365730, 11.4-STABLE before r365738, 12.1-RELEASE before p10, 11.4-RELEASE before p4, and 11.3-RELEASE before p14, a programming error in the ure(4) device driver caused some Realtek USB Ethernet interfaces to incorrectly report packets with more than 2048 bytes in a single USB transfer as having a length of only 2048 bytes. An adversary can exploit this to cause the driver to misinterpret part of the payload of a large packet as a separate packet, and thereby inject packets across security boundaries such as VLANs.

CVE-2020-25578

In FreeBSD 12.2-STABLE before r368969, 11.4-STABLE before r369047, 12.2-RELEASE before p3, 12.1-RELEASE before p13 and 11.4-RELEASE before p7 several file systems were not properly initializing the d_off field of the dirent structures returned by VOP_READDIR. In particular, tmpfs(5), smbfs(5), autofs(5) and mqueuefs(5) were failing to do so. As a result, eight uninitialized kernel stack bytes may be leaked to userspace by these file systems. 5.3 MEDIUM

CVE-2020-25579

In FreeBSD 12.2-STABLE before r368969, 11.4-STABLE before r369047, 12.2-RELEASE before p3, 12.1-RELEASE before p13 and 11.4-RELEASE before p7 msdosfs(5) was failing to zero-fill a pair of padding fields in the dirent structure, resulting in a leak of three uninitialized bytes.

Fixed security vulnerabilities in R6628P35

CVE-1999-0524

ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

CVE-2022-0778

A flaw was found in OpenSSL. It is possible to trigger an infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens before verification of the certificate signature, any process that parses an externally supplied certificate may be subject to a denial of service attack

CVE-2021-40490

A race condition was discovered in `ext4_write_inline_data_end` in `fs/ext4/inline.c` in the `ext4` subsystem in the Linux kernel through 5.13.13.

CVE-2021-20317

A flaw was found in the Linux kernel. A corrupted timer tree caused the task wakeup to be missing in the `timerqueue_add` function in `lib/timerqueue.c`. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP.

CVE-2021-3679

A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with `CAP_SYS_ADMIN` capability) could use this flaw to starve the resources causing denial of service.

CVE-2021-4160

There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc-dev (Affected 1.0.2-1.0.2zb).

CNVD-2019-23102/CVE-2019-10638/HSVD-202103-0

In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.

CVE-2020-10188

`utility.c` in `telnetd` in `netkit telnet` through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the `netclear` and `nextitem` functions.

CVE-1999-0511

IP forwarding is enabled on a machine which is not a router or firewall.

Fixed security vulnerabilities in R6615P07

None

Appendix C Upgrading software

This chapter describes types of software used on the switch and how to upgrade software while the switch is operating normally or when the switch 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 minimum modules required for device operation and some basic features, including device management, interface management, configuration management, and routing management.

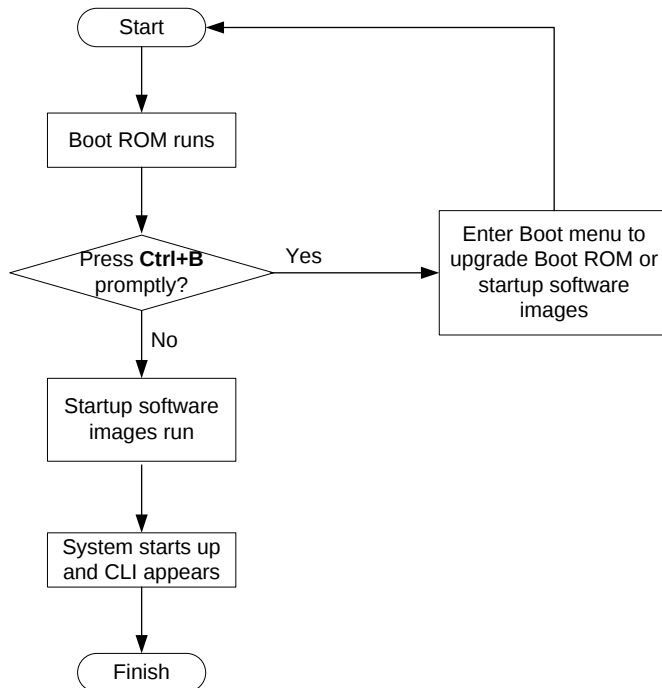
The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

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**.

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	- Boot ROM image - Software images	- You must reboot the switch to complete the upgrade. - This method can interrupt ongoing network services.
Upgrading from the Boot menu	- Boot ROM image - Software images	Use this method when the switch cannot correctly start up. ⚠ CAUTION: Upgrading an IRF fabric from the CLI instead of the Boot menu. The Boot menu method increases the service downtime, because it requires that you upgrade the member switches one by one.

The output in this document is for illustration only and might vary with software releases. This document uses `boot.bin` and `system.bin` to represent boot and system image names. The actual software image name format is `chassis-model_Comware-version_image-type_release`, for example, `5140HI-CMW710-BOOT-Rxxxx.bin` and `5140HI-CMW710-SYSTEM-Rxxxx.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. For more information about setting up and configuring an IRF fabric, see the installation guide and IRF configuration guide for the HPE 5130 EI switch series.

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. 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. Verify that each IRF member switch has sufficient storage space for the upgrade images.

IMPORTANT:

Each IRF member switch must have free storage space that is at least two times the size of the upgrade image file.

Identify the free flash space of the master switch.

```
<Sysname> dir
```

Directory of flash:

0	-rw-	41424	Aug 23 2013 02:23:44	startup.mdb
1	-rw-	3792	Aug 23 2013 02:23:44	startup.cfg
2	-rw-	53555200	Aug 23 2013 09:53:48	system.bin
3	drw-	-	Aug 23 2013 00:00:07	seclog
4	drw-	-	Aug 23 2013 00:00:07	diagfile
5	drw-	-	Aug 23 2013 00:00:07	logfile
6	-rw-	9959424	Aug 23 2013 09:53:48	boot.bin
7	-rw-	9012224	Aug 23 2013 09:53:48	backup.bin

524288 KB total (453416 KB free)

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

```
<Sysname> dir slot2#flash:/
```

Directory of slot2#flash:/

0	-rw-	41424	Jan 01 2011 02:23:44	startup.mdb
---	------	-------	----------------------	-------------

1	-rw-	3792	Jan 01 2011 02:23:44	startup.cfg
2	-rw-	93871104	Aug 23 2013 16:00:08	system.bin
3	drw-	-	Jan 01 2011 00:00:07	seclog
4	drw-	-	Jan 01 2011 00:00:07	diagfile
5	drw-	-	Jan 02 2011 00:00:07	logfile
6	-rw-	13611008	Aug 23 2013 15:59:00	boot.bin
7	-rw-	9012224	Nov 25 2011 09:53:48	backup.bin

524288 KB total (453416 KB free)

4. 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.
5. Delete unused files in the flash memory to free space:

CAUTION:

- To avoid data loss, do not delete the current configuration file. For information about the current configuration file, use the **display startup** command.
- The **delete /unreserved file-url** command deletes a file permanently and the action cannot be undone.
- The **delete file-url** command moves a file to the recycle bin and the file still occupies storage space. To free the storage space, first execute the **undelete** command to restore the file, and then execute the **delete /unreserved file-url** command.

```
# Delete unused 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.

# Delete unused 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 images to the master switch

Before you start upgrading software images 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](#)

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. Execute 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+C to abort
```

```
Connected to 10.10.110.1(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. Execute 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.
```

```
32133120 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:

On the IRF fabric:

1. Enable FTP server.

```
<Sysname> system-view
```

```
[Sysname] ftp server enable
```

2. Configure a local FTP user account:

```
# Create the user account.
```

```
[Sysname] local-user abc
```

```
# Set its password and specify the FTP service.
```

```
[Sysname-luser-manage-abc] password simple pwd
```

```
[Sysname-luser-manage-abc] service-type ftp
```

```
# Assign the network-admin user role to the user account for uploading file to the working directory of the server.
```

```
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
```

```
[Sysname-luser-manage-abc] quit
```

```
[Sysname] quit
```

On the PC:

3. Log in to the IRF fabric (the FTP server) in FTP mode.

```
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.

```

4. Enable the binary file transfer mode.

```

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

```

5. Upload the file (for example, **newest.ipe**) to the root directory of the flash memory on the master switch.

```

ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 32133120 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, execute the tftp command in user view to download the file to the root directory of the flash memory on 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 30.6M	0 30.6M	0 0	143k 0	--:--:--	0:03:38	--:--:--	142k

Upgrading the software images

To upgrade the software images:

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

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
```

Verifying image file.....Done.

Images in IPE:

```

boot.bin
system.bin

```

This command will set the main startup software images. Continue? [Y/N]:y

Add images to target slot.

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

Decompressing file system.bin to flash:/system.bin.....Done.

The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 1.

2. Specify the upgrade image file as the main startup image file for each subordinate switch. This example uses IRF member 2. (The subordinate switches will automatically copy the file to the root directory of their flash memories.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
```

Verifying image file.....Done.

Images in IPE:

boot.bin
system.bin

This command will set the main startup software images. Continue? [Y/N]:y

Add images to target slot.

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

Decompressing file system.bin to flash:/system.bin.....Done.

The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 2.

3. Enable the software auto-update function.

<Sysname> system-view

[Sysname] irf auto-update enable

[Sysname] quit

This function checks the software versions of member switches for inconsistency with the master switch. If a subordinate switch is using a different software version than the master, the function propagates the current software images of the master to the subordinate as main startup images. The function prevents software version inconsistency from causing the IRF setup 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. Execute 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 upgrade 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.

Upgrading 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.

**TIP:**

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

Prerequisites

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

Setting up the upgrade environment

1. Use a console cable to connect the console terminal (for example, a PC) to the console port on the switch.
2. Connect the Ethernet port on the switch to the file server.

NOTE:

The file server and the configuration terminal can be co-located.

3. 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

Preparing for the TFTP or FTP transfer

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 the file server and the switch can reach each other.

Verifying that sufficient storage space is available

**IMPORTANT:**

For the switch to start up correctly, do not delete the main startup software images when you free storage space before upgrading Boot ROM. On the Boot menu, the main startup software images are marked with an asterisk (*).

When you upgrade software, make sure each member switch has sufficient free storage space for the upgrade file, as shown in [Table 9](#).

Table 9 Minimum free storage space requirements

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.

Upgraded images	Minimum free storage space requirements
Boot ROM	Same size as the Boot ROM upgrade image file.

If no sufficient space is available, delete unused files as described in “[Managing files from the Boot menu.](#)”

Scheduling the upgrade time

During the upgrade, the switch cannot provide any services. You must make sure the upgrade has a minimal impact on the network services.

Accessing the Boot menu

```
Starting.....
Press Ctrl+D to access BASIC BOOT MENU
*****
*
*          HPE 5140 48G 4SFP+ 1-slot HI Sw B00TROM, Version 117
*
*****
Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP

Creation Date       : Nov 10 2020, 10:01:13
CPU Clock Speed    : 800MHz
Memory Size        : 2048MB
Flash Size         : 512MB
CPLD Version       : 002
PCB Version        : Ver.B
Mac Address        : 000fe2699a00
```

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

Press one of the shortcut key combinations at prompt.

Table 10 Shortcut keys

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

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 117
*
*****
```

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 11 Basic Boot ROM menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port .
2. Update extended BootRom	Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port .
3. Update basic BootRom	Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port .
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see Accessing the extended Boot menu .
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press Ctrl + U to access the BASIC ASSISTANT menu (see Table 12).

Table 12 BASIC ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.

Option	Task
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 13](#)). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 5130 EI Switch Series Configuration Guides*.

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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

```

Enter your choice(0-8):

Table 13 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	- Specify the main and backup software image file for the next startup. - Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.

Option	Tasks
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+R: Download image to SDRAM and run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 14 .
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

Table 14 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.

Upgrading Comware images from the Boot menu

You can use the following methods to upgrade Comware images:

- [Using TFTP to upgrade software images through the Ethernet port](#)
- [Using FTP to upgrade software images through the Ethernet port](#)
- [Using XMODEM to upgrade software through the console port](#)

Using TFTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.
 1. Set TFTP protocol parameters
 2. Set FTP protocol parameters
 3. Set XMODEM protocol parameters
 0. Return to boot menu

Enter your choice(0-3):

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

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

Table 15 TFTP parameter description

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

NOTE:

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

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

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

4. Enter **Y** to start downloading the image file. To return to the Boot menu without downloading the upgrade file, 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 with the main images first. 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 only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
 - If an image with the same attribute as the image you are loading is already in the 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

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8): 0

Using FTP to upgrade software images through the 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 16 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, update.ipe).

Item	Description
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 without downloading the upgrade file, 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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

```

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

NOTE:

- The switch always attempts to boot with the main images first. 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 only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
 - If an image with the same attribute as the image you are loading is already in the 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 Ethernet port. To save time, use the 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.

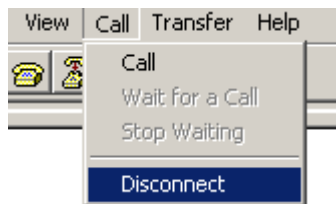
```
Download baudrate is 115200 bps
```

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

```
Press enter key when ready
```

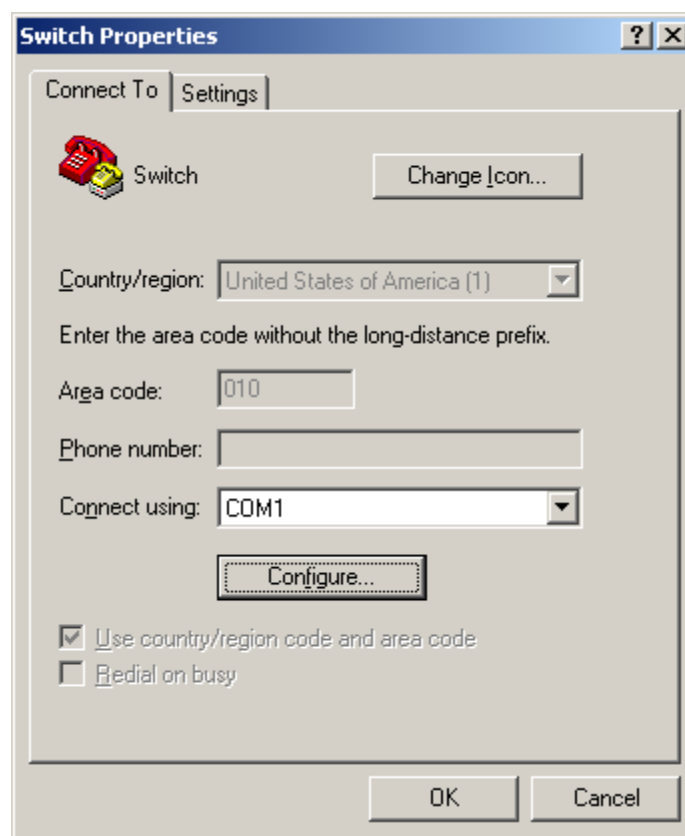
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
 - a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



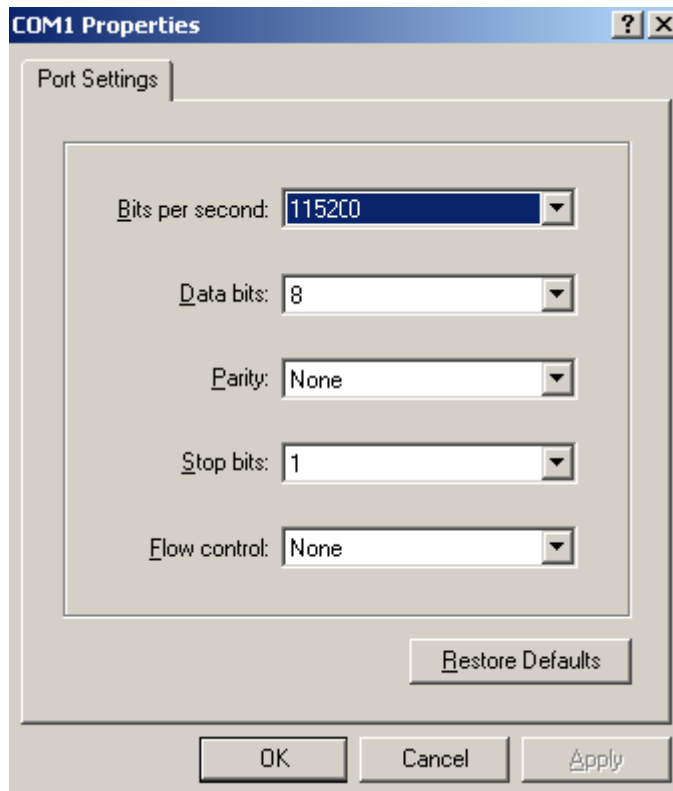
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



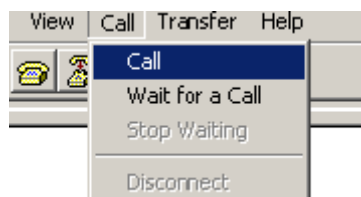
- c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 4 Modifying the baud rate



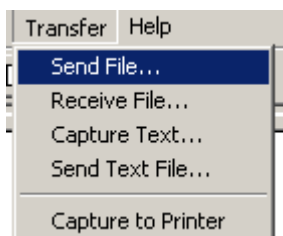
- d. Select **Call** > **Call** to reestablish the connection.

Figure 5 Reestablishing the connection



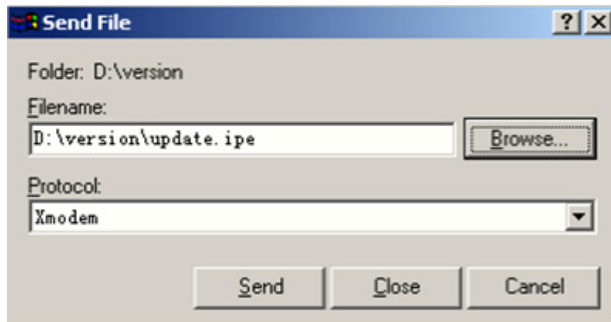
5. Press **Enter**. The following prompt appears:
Are you sure to download file to flash? Yes or No (Y/N):Y
6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCC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

Figure 6 Transfer menu



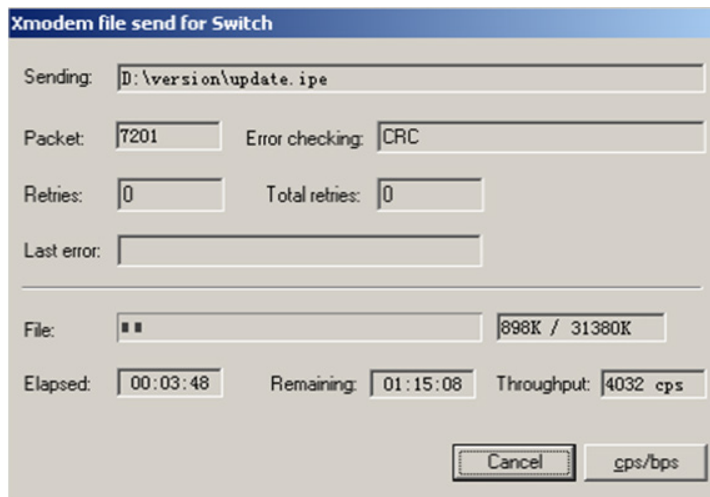
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box



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

Figure 8 File transfer progress



10. 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 (At the prompt,

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 with the main images first. 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 only stored in the flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
 - 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.
-

- 11.** If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps as described in step 5.a. If the baud rate is 9600 bps, skip this step.
-

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright
```

Enter your choice(0-8): 0

- 12.** Enter **0** in the Boot menu to reboot the system with the new software images.

Upgrading Boot ROM from the Boot menu

You can use the following methods to upgrade the Boot ROM image:

- [Using TFTP to upgrade Boot ROM through the Ethernet port](#)
- [Using FTP to upgrade Boot ROM through the Ethernet port](#)
- [Using XMODEM to upgrade Boot ROM through the console port](#)

Using TFTP to upgrade Boot ROM through the 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 17 TFTP parameter description

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

NOTE:

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

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 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 :123

Table 18 FTP parameter description

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

NOTE:

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

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 Ethernet port. To save time, use the 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

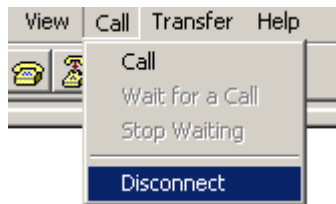
Enter your choice(0-3):

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.

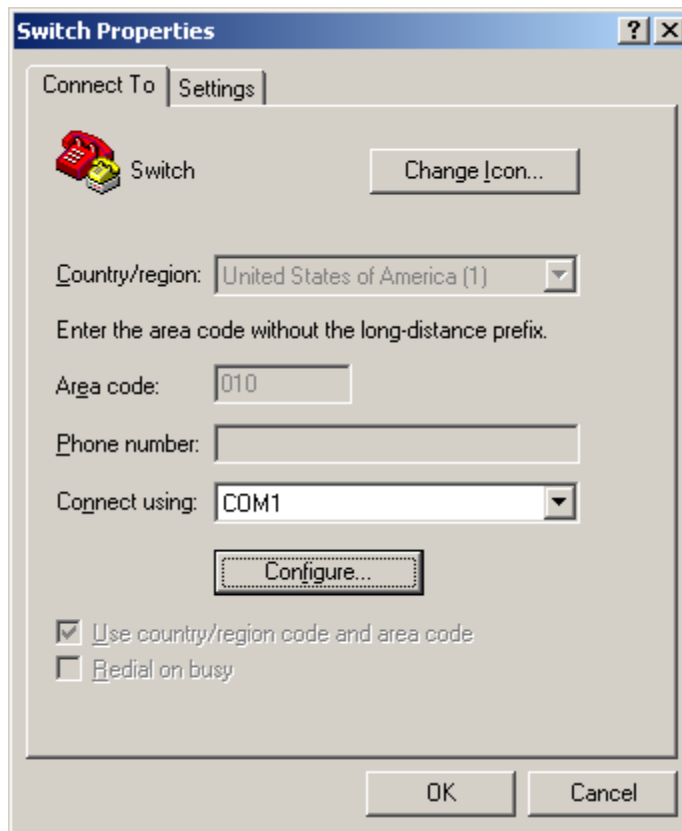
- a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



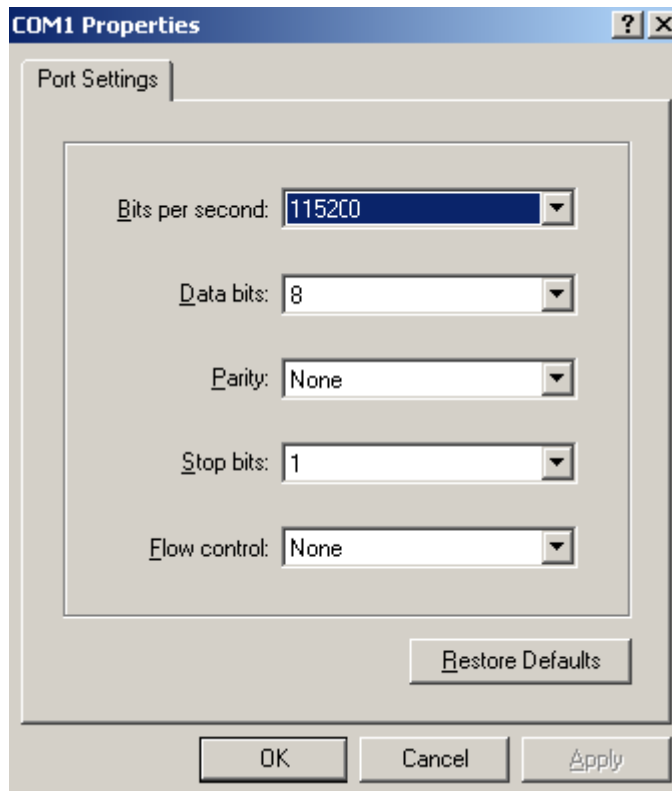
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



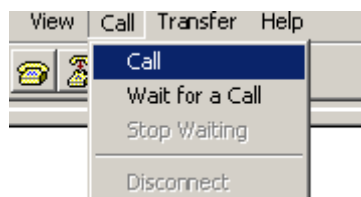
- c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



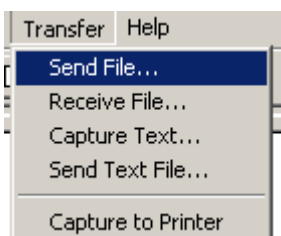
- d. Select **Call > Call** to reestablish the connection.

Figure 12 Reestablishing the connection



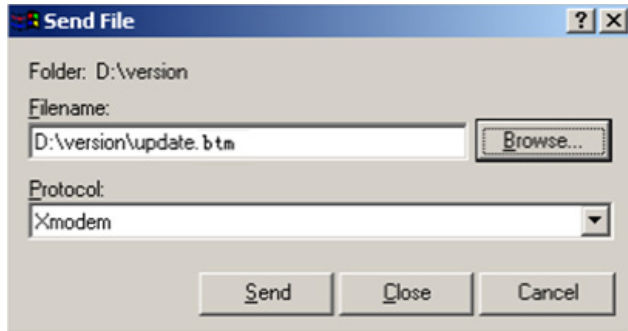
6. Press **Enter** to start downloading the file.
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
7. Select **Transfer > Send File** in the HyperTerminal window.

Figure 13 Transfer menu



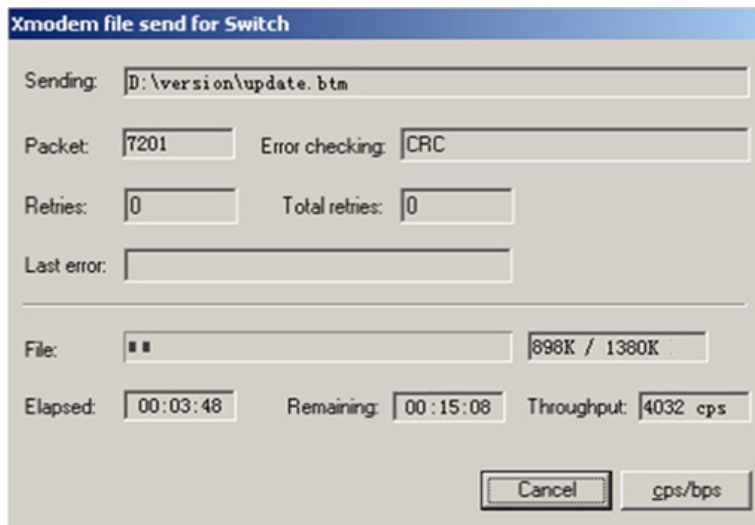
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 14 File transmission dialog box



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

Figure 15 File transfer progress



10. 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.
11. Enter **Y** at the prompt to upgrade the extended Boot ROM section.
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.....Done.
12. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps at the prompt, as described in step 4.a. If the baud rate is 9600 bps, skip this step.
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

13. Press **Enter** to access the Boot ROM update menu.
14. 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):

15. 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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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: 464298848 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: 464298848 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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

Enter your choice(0-8): 2

2. **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: 417177920 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 5140HI-CMW710-R6652P05

Release Notes

Software Feature Changes

Contents

R6652P05.....	1
Modified feature: Specifying the cipher suite for MACsec encryption.....	1
Feature change description.....	1
Command changes.....	1
Modified command: macsec cipher-suite.....	1
Modified feature: Displaying BGP dedicated routing information.....	1
Feature change description.....	1
R6652P03.....	1
New feature: Specifying the cipher suite for MACsec encryption	1
Specifying the cipher suite for MACsec encryption.....	1
Command reference	1
macsec cipher-suite	1
R6628P43.....	1
R6628P40.....	2
R6628P35.....	3
New feature: Enabling packet statistics for a Layer 3 aggregate subinterface.....	3
Enabling packet statistics for a Layer 3 aggregate subinterface.....	3
Command reference	4
traffic-statistic enable	4
New feature: Object groups	4
Configuring object groups	4
Configuring an IPv4 address object group	4
Configuring an IPv6 address object group	5
Configuring a port object group.....	5
Configuring a service object group.....	5
Display and maintenance commands for object groups	6
Command reference	6
description.....	6
display object-group	6
network (IPv4 address object group view)	8
network (IPv6 address object group view)	9
object-group	10
port (port object group view)	11
service (service object group view)	13
Modified feature: Applying a QoS policy to an interface	15
Feature change description.....	15
Command changes.....	15
Modified feature: Configuring the authentication load sharing mode for users attached to DRNI interfaces.....	15
Feature change description.....	15
Command changes	16
Modified command: port-security drni load-sharing-mode.....	16

Modified feature: Setting the maximum number of configuration archives for local archiving	16
Feature change description.....	16
Command changes	16
Modified command: archive configuration max.....	16
Modified feature: Displaying detailed next hop information in the RIB or for direct routes or static routes.....	16
Feature change description.....	16
Command changes	17
Modified command: display rib nib.....	17
Modified command: display route-direct nib.....	17
Modified command: display ipv6 rib nib	18
Modified command: display ipv6 route-direct nib	18
Modified command: display route-static nib	18
Modified command: display ipv6 route-static nib	19
Modified feature: Optimizing BMP server information display	19
Feature change description.....	19
Command changes	20
Modified command: display bgp bmp server.....	20
Modified feature: Setting the 802.1X periodic reauthentication timer	20
Feature change description.....	20
Command changes	21
Modified command: dot1x timer reauth-period (interface view)	21
Modified command: dot1x timer	21
Modified feature: Setting the periodic MAC reauthentication timer	22
Feature change description.....	22
Command changes	22
Modified command: mac-authentication timer (interface view)	22
Modified command: mac-authentication timer (system view)	22
Modified feature: Displaying local public keys.....	23
Feature change description.....	23
Command changes	23
Modified command: display public-key local public.....	23
Modified feature: Value range for the ID of an IPsec tunnel	23
Feature change description.....	23
Command changes	23
Modified command: display ipsec statistics	23
Modified command: display ipsec tunnel	23
Modified command: reset ipsec statistics.....	24
Modified feature: Configuring automatic email sending parameters for an EAA monitor policy	24
Feature change description.....	24
Command changes	24
Modified command: rtm email domain	24
Modified feature: Setting the usage alarm threshold of a log file	24
Feature change description.....	24
Command changes	25
Modified command: info-center logfile alarm-threshold	25
Modified feature: Displaying heap memory usage for a user process	25
Feature change description.....	25

Command changes	25
Modified command: display process memory heap	25
Modified feature: Displaying gRPC information	25
Feature change description	25
Command changes	26
R6615P07	27
Removed feature: Enabling the SSH server to support SSH1 clients	27
Feature change description	27
Deleted command	27
ssh server compatible-ssh1x enable	27
Removed feature: Setting the minimum interval for updating the RSA server key pair	27
Feature change description	27
Deleted command	27
ssh server rekey-interval	27
R6615P06	28

R6652P05

This software version has the following changes:

- [Modified feature: Specifying the cipher suite for MACsec encryption](#)
- [Modified feature: Displaying BGP dedicated routing information](#)

Modified feature: Specifying the cipher suite for MACsec encryption

Feature change description

Added support for the standard GCM-AES-256 and GCM-AES-XPB-256 cipher suites.

Command changes

Modified command: `macsec cipher-suite`

Old syntax

```
macsec cipher-suite { gcm-aes-128 | gcm-aes-256 | gcm-aes-xpn-128 |  
gcm-aes-xpn-256 }
```

New syntax

```
macsec cipher-suite { gcm-aes-128 | gcm-aes-256 [ standard ] |  
gcm-aes-xpn-128 | gcm-aes-xpn-256 [ standard ] }
```

Views

Ethernet interface view

Change description

The **standard** keyword was added to the `macsec cipher-suite` command.

standard: Specifies the standard cipher suite. H3C's GCM-AES-256 and GCM-AES-XPB-256 cipher suites differ from the standard open source GCM-AES-256 and GCM-AES-XPB-256 cipher suites in implementation, respectively. To successfully establish MKA sessions with a peer using the standard open source GCM-AES-256 or GCM-AES-XPB-256 cipher suite for MACsec encryption, you must specify the **standard** keyword in the `macsec cipher-suite` command.

Modified feature: Displaying BGP dedicated routing information

Feature change description

The **S – stale** route state is added to the output from the `display bgp routing-table dedicated` command. This state indicates stale routes.

R6652P03

This release has the following changes:

- [New feature: Specifying the cipher suite for MACsec encryption](#)

New feature: Specifying the cipher suite for MACsec encryption

Specifying the cipher suite for MACsec encryption

About this task

MACsec uses the GCM-AES-128 or GCM-AES-256 cipher suite to encrypt, validate, and decrypt protected data frames.

Restrictions and guidelines

Only the HPE FlexNetwork 5140/5520 10GBASE-T MACsec 2p Mod (R9L65A) modules support the GCM-AES-256 cipher suite.

This feature is supported only in device-oriented mode. Do not configure this feature on an 802.1X-enabled port.

Make sure the connected MACsec ports are configured with the same cipher suite. If the ports are configured with different cipher suites, they cannot successfully establish MKA sessions.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Specify the cipher suite for MACsec encryption.
macsec cipher-suite { gcm-aes-128 | gcm-aes-256 }
By default, MACsec uses the GCM-AES-128 cipher suite for encryption.

Command reference

macsec cipher-suite

Use **macsec cipher-suite** to specify the cipher suite for MACsec encryption.

Use **undo macsec cipher-suite** to restore the default.

Syntax

```
macsec cipher-suite { gcm-aes-128 | gcm-aes-256 }  
undo macsec cipher-suite
```

Default

MACsec uses the GCM-AES-128 cipher suite for encryption.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

gcm-aes-128: Specifies the GCM-AES-128 cipher suite.

gcm-aes-256: Specifies the GCM-AES-256 cipher suite.

Usage guidelines

Only the HPE FlexNetwork 5140/5520 10GBASE-T MACsec 2p Mod (R9L65A) modules support the GCM-AES-256 cipher suite.

Do not use this command on an 802.1X-enabled port.

This command is supported only in device-oriented mode. Make sure the connected ports are configured with the same cipher suite. If the ports are configured with different cipher suites, they cannot successfully establish MKA sessions.

Examples

```
# Specify the GCM-AES-256 cipher suite for MACsec encryption on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] macsec cipher-suite gcm-aes-256
```

R6628P43

This release has no feature changes.

R6628P40

This release has no feature changes.

R6628P35

This software version has the following changes:

- New feature: Enabling packet statistics for a Layer 3 aggregate subinterface
- New feature: Object groups
- Modified feature: Applying a QoS policy to an interface
- Modified feature: Configuring the authentication load sharing mode for users attached to DRNI interfaces
- Modified feature: Setting the maximum number of configuration archives for local archiving
- Modified feature: Displaying detailed next hop information in the RIB or for direct routes or static routes
- Modified feature: Optimizing BMP server information display
- Modified feature: Setting the 802.1X periodic reauthentication timer
- Modified feature: Setting the periodic MAC reauthentication timer
- Modified feature: Displaying local public keys
- Modified feature: Value range for the ID of an IPsec tunnel
- Modified feature: Configuring automatic email sending parameters for an EAA monitor policy
- Modified feature: Setting the usage alarm threshold of a log file
- Modified feature: Displaying heap memory usage for a user process
- Modified feature: Displaying gRPC information

New feature: Enabling packet statistics for a Layer 3 aggregate subinterface

Enabling packet statistics for a Layer 3 aggregate subinterface

Restrictions and guidelines

The packet statistics feature is CPU intensive. When you use this command for Layer 3 aggregate subinterfaces, make sure you fully understand its impact on system performance. You can use the **flow-interval** command to adjust the interval at which the statistics are polled. To conserve hardware resources, increase the polling interval.

Procedure

1. Enter system view.
system-view
2. Enter Layer 3 aggregate subinterface view.
interface route-aggregation *interface-number.subnumber*
3. Enable packet statistics for the Layer 3 aggregate subinterface.
traffic-statistic enable
By default, the packet statistics feature is disabled for a Layer 3 aggregate subinterface.
4. (Optional.) Display the packet statistics for the Layer 3 aggregate subinterface.
display interface

In the command output, the **Input** and **Output** fields display packet statistics.

Command reference

traffic-statistic enable

Use **traffic-statistic enable** to enable packet statistics for a Layer 3 aggregate subinterface.

Use **undo traffic-statistic enable** to disable packet statistics for a Layer 3 aggregate subinterface.

Syntax

traffic-statistic enable

undo traffic-statistic enable

Default

The packet statistics feature is disabled for a Layer 3 aggregate subinterface.

Views

Layer 3 aggregate subinterface view

Predefined user roles

network-admin

Usage guidelines

The packet statistics feature is CPU intensive. When you use this command for Layer 3 aggregate subinterfaces, make sure you fully understand its impact on system performance. You can use the **flow-interval** command to adjust the interval at which the statistics are polled. To conserve hardware resources, increase the polling interval.

To view packet statistics of Layer 3 aggregate subinterfaces, use the **display interface** command.

Examples

```
# Enable packet statistics for Layer 3 aggregate subinterface Route-Aggregation 1.1.
<Sysname> system-view
[Sysname] interface route-aggregation 1.1
[Sysname-Route-Aggregation1.1] traffic-statistic enable
```

Related commands

display interface

flow-interval

New feature: Object groups

Configuring object groups

Configuring an IPv4 address object group

1. Enter system view.
system-view

2. Configure an IPv4 address object group and enter its view.
object-group ip address *object-group-name*
The system has one default IPv4 address object group named **any**.
3. (Optional.) Configure a description for the IPv4 address object group.
description *text*
By default, an object group does not have a description.
4. Configure an IPv4 address object.
[*object-id*] **network** { **host** { **address** *ip-address* | **name** *host-name* } | **subnet** *ip-address* { *mask-length* | *mask* } }

Configuring an IPv6 address object group

1. Enter system view.
system-view
2. Configure an IPv6 address object group and enter its view.
object-group ipv6 address *object-group-name*
The system has one default IPv6 address object group named **any**.
3. (Optional.) Configure a description for the IPv6 address object group.
description *text*
By default, an object group does not have a description.
4. Configure an IPv6 address object.
[*object-id*] **network** { **host** { **address** *ipv6-address* | **name** *host-name* } | **subnet** *ipv6-address* *prefix-length* }

Configuring a port object group

1. Enter system view.
system-view
2. Configure a port object group and enter its view.
object-group port *object-group-name*
The system has one default port object group named **any**.
3. (Optional.) Configure a description for the port object group.
description *text*
By default, an object group does not have a description.
4. Configure a port object.
[*object-id*] **port** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* }

Configuring a service object group

1. Enter system view.
system-view
2. Configure a service object group and enter its view.
object-group service *object-group-name*
The system has multiple default service object groups.
3. (Optional.) Configure a description for the service object group.
description *text*

By default, an object group does not have a description.

4. Configure a service object.

```
[ object-id ] service { protocol [ { source { { eq | lt | gt } port | range port1 port2 } | destination { { eq | lt | gt | } port | range port1 port2 } } * | icmp-type icmp-code | icmpv6-type icmpv6-code ] }
```

Display and maintenance commands for object groups

Execute **display** commands in any view.

Task	Command
Display information about object groups.	display object-group [{ { ip ipv6 } address service port } [default] [name object-group-name] name object-group-name]

Command reference

description

Use **description** to configure a description for an object group.

Use **undo description** to restore the default.

Syntax

description text

undo description

Default

No description is configured for an object group.

Views

Object group view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

Configure the description as **This is an IPv4 object-group** for an IPv4 address object group.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] description This is an IPv4 object-group
```

display object-group

Use **display object-group** to display information about object groups.

Syntax

```
display object-group [ { { ip | ipv6 } address | service | port } [ default ]  
[ name object-group-name ] | name object-group-name ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip address: Specifies the IPv4 address object groups.

ipv6 address: Specifies the IPv6 address object groups.

port: Specifies the port object groups.

service: Specifies the service object groups.

default: Specifies the default object groups.

name *object-group-name*: Specifies an object group by its name, a case-insensitive string of 1 to 31 characters.

Examples

```
# Display information about all object groups.  
<Sysname> display object-group  
IP address object group obj1: 0 object(in use)  
IP address object group obj2: 7 objects(out of use)  
0 network host address 1.1.1.1  
10 network host name host  
20 network subnet 1.1.1.1 255.255.255.0  
IPv6 address object-group obj3: 0 object(in use)  
IPv6 address object-group obj4: 5 objects(out of use)  
0 network host address 1::1:1  
10 network host name host  
20 network subnet 1::1:0 112  
Service object-group obj5: 0 object(in use)  
Service object-group obj6: 6 objects(out of use)  
0 service 200  
10 service tcp source lt 50 destination range 30 40  
20 service udp source range 30 40 destination gt 30  
30 service icmp 20 20  
40 service icmpv6 20 20  
Port object-group obj7: 0 object(in use)  
Port object-group obj8: 3 objects(out of use)  
0 port lt 20  
10 port range 20 30  
  
# Display information about object group obj2.  
<Sysname> display object-group name obj2  
IP address object-group obj2: 6 objects(out of use)  
0 network host address 1.1.1.1
```

```

10 network host name host
20 network subnet 1.1.1.1 255.255.255.0

# Display information about all IPv4 address object groups.
<Sysname> display object-group ip address
IP address object-group obj1: 0 object(in use)
IP address object-group obj2: 6 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0

# Display information about IPv6 address object group obj4.
<Sysname> display object-group ipv6 address name obj4
IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112

```

Table 1 Command output

Field	Description
in use	The object group is used by an ACL or object group.
out of use	The object group is not used.

network (IPv4 address object group view)

Use **network** to configure an IPv4 address object.

Use **undo network** to delete an IPv4 address object.

Syntax

```

[ object-id ] network { host { address ip-address | name host-name } | subnet
ip-address { mask-length | mask } }

undo network { host { address ip-address | name host-name } | subnet
ip-address { mask-length | mask } }

undo object-id

```

Default

No IPv4 address objects exist.

Views

IPv4 address object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv4 address object with the host address or name.

address ip-address: Specifies an IPv4 host address.

name *host-name*: Specifies a host name, a case-insensitive string of 1 to 60 characters.

subnet *ip-address* { *mask-length* | *mask* }: Configures an IPv4 address object with the subnet address followed by a mask length in the range of 0 to 32 or a mask in dotted decimal notation.

Usage guidelines

This command fails if you use it to configure or change an IPv4 address object to be identical with an existing object.

This command creates an IPv4 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet with the mask length of 32 or the mask of 255.255.255.255, the system configures the object with a host address.

Examples

Configure an IPv4 address object with the host address of **192.168.0.1**.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] network host address 192.168.0.1
```

Configure an IPv4 address object with the host name of **pc3**.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] network host name pc3
```

Configure an IPv4 address object with the IPv4 address of **192.167.0.0** and mask length of **24**.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] network subnet 192.167.0.0 24
```

Configure an IPv4 address object with the IPv4 address of **192.166.0.0** and mask of **255.255.0.0**.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] network subnet 192.166.0.0 255.255.0.0
```

network (IPv6 address object group view)

Use **network** to configure an IPv6 address object.

Use **undo network** to delete an IPv6 address object.

Syntax

```
[ object-id ] network { host { address ipv6-address | name host-name } | subnet ipv6-address prefix-length }
```

```
undo network { host { address ipv6-address | name host-name } | subnet ipv6-address prefix-length }
```

```
undo object-id
```

Default

No IPv6 address objects exist.

Views

IPv6 address object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not configure an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv6 address object with the host address or name.

address ipv6-address: Specifies an IPv6 host address.

name host-name: Specifies a host name, a case-insensitive string of 1 to 60 characters.

subnet ipv6-address prefix-length: Configures an IPv6 address object with the subnet address followed by the prefix length in the range of 1 to 128.

Usage guidelines

This command fails if you use it to configure or change an IPv6 address object to be identical with an existing object.

This command creates an IPv6 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet address with the prefix length of 128, the system configures the object with a host address.

Examples

Configure an IPv6 address object with the host address of **1::1**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host address 1::1
```

Configure an IPv6 address object with the host name of **pc3**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host name pc3
```

Configure an IPv6 address object with the IPv6 address of **1:1:1::1** and prefix length of **24**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ip v6group] network subnet 1:1:1::1 24
```

object-group

Use **object-group** to configure an object group and enter its view, or enter the view of an existing object group.

Use **undo object-group** to delete an object group.

Syntax

```
object-group { { ip | ipv6 } address | port | service } object-group-name
undo object-group { { ip | ipv6 } address | port | service }
object-group-name
```

Default

Default object groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

ip address: Configures an IPv4 address object group.

ipv6 address: Configures an IPv6 address object group.

port: Configures a port object group.

service: Configures a service object group.

object-group-name: Specifies an object group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The **object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system creates a new object group and enters the object group view.
- If the specified group exists but the group type is different from that in the command, the command fails.

The **undo object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system executes the command without any system prompt.
- If the specified group exists and the group type is the same as that in the command, the system deletes the group.
- If the specified group exists but the group type is different from that in the command, the command fails.
- If the specified object group is being used by an ACL, object policy, or object group, the command fails.

Default object groups cannot be deleted.

Examples

Configure an IPv4 address object group named **ipgroup**.

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

Configure an IPv6 address object group named **ipv6group**.

```
<Sysname> system-view
```

```
[Sysname] object-group ipv6 address ipv6group
```

Configure a port object group named **portgroup**.

```
<Sysname> system-view
```

```
[Sysname] object-group port portgroup
```

Configure a service object group named **servicegroup**.

```
<Sysname> system-view
```

```
[Sysname] object-group service servicegroup
```

port (port object group view)

Use **port** to configure a port object.

Use **undo port** to delete a port object.

Syntax

```
[ object-id ] port { { eq | lt | gt } port | range port1 port2 }  
undo port { { eq | lt | gt } port | range port1 port2 }  
undo object-id
```

Default

No port objects exist.

Views

Port object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

eq: Configures a port object with a port number equal to the specified port.

lt: Configures a port object with a port number smaller than the specified port.

gt: Configures a port object with a port number greater than the specified port.

port: Specifies a port number in the range of 0 to 65535.

range *port1 port2*: Configures a port object with a port range. The value range for the *port1* and *port2* arguments is 0 to 65535.

Usage guidelines

This command fails if you use it to configure or change a port object to be identical with an existing object.

This command creates a port object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **lt** *port* option, follow these guidelines:

- The value of *port* cannot be 0.
- If the value of *port* is 1, the system configures the object with a port number of 0.
- If the value of *port* is in the range of 2 to 65535, the system configures the object with a port number range of [0, *port*-1].

When you use the **gt** *port* option, follow these guidelines:

- The value of *port* cannot be 65535.
- If the value of *port* is 65534, the system configures the object with a port number of 65535.
- If the value of *port* is in the range of 0 to 65533, the system configures the object with a port number range of [*port*+1, 65535].

When you use the **range** *port1 port2* option, follow these guidelines:

- If *port1* is equal to *port2*, the system configures the object with the port number *port1*.
- If *port1* is smaller than *port2*, the system configures the object with the port number range.
- If *port1* is greater than *port2*, the system changes the range to [*port2*, *port1*] and configures the object with the changed port number range.

- If *port1* is 0, the range is displayed as **lt port2+1**.
- If *port2* is 65535, the range is displayed as **gt port1-1**.

Examples

```
# Configure a port object with a port number of 100.
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port eq 100

# Configure a port object with a port number smaller than 20.
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port lt 20

# Configure a port object with a port number greater than 60000.
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port gt 60000

# Configure a port object with a port number in the range of 1000 to 2000.
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port range 1000 2000
```

service (service object group view)

Use **service** to configure a service object.

Use **undo service** to delete a service object.

Syntax

```
[ object-id ] service { protocol [ { source { { eq | lt | gt } port | range port1 port2 } | destination { { eq | lt | gt } port | range port1 port2 } } * | icmp-type icmp-code | icmpv6-type icmpv6-code ] }

undo service { protocol [ { source { { eq | lt | gt } port | range port1 port2 } | destination { { eq | lt | gt } port | range port1 port2 } } * | icmp-type icmp-code | icmpv6-type icmpv6-code ] }

undo object-id
```

Default

No service objects exist.

Views

Service object group view

Predefined user roles

network-admin

Parameters

object-id: Configures an object ID in the range of 0 to 4294967294. If you do not configure an ID for the object, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the automatically assigned ID is 30.

protocol: Configures the protocol number in the range of 0 to 255, or the protocol name such as TCP, UDP, ICMP, and ICMPv6.

source: Configures a service object with a source port when the protocol is TCP or UDP.

destination: Configures a service object with a destination port when the protocol is TCP or UDP.

eq: Configures a port equal to the specified port.

lt: Configures a port smaller than the specified port.

gt: Configures a port greater than the specified port.

port: Specifies a port number in the range of 0 to 65535.

range port1 port2: Configures a service object with a port range. The value range for the *port1* and *port2* arguments is 0 to 65535.

icmp-type: Configures the ICMP message type in the range of 0 to 255.

icmp-code: Configures the ICMP message code in the range of 0 to 255.

icmpv6-type: Configures the ICMPv6 message type in the range of 0 to 255.

icmpv6-code: Configures the ICMPv6 message code in the range of 0 to 255.

Usage guidelines

This command fails if you use it to configure or change a service object to be identical with an existing object.

This command creates a service object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **lt port** option, follow these guidelines:

- The value of *port* cannot be 0.
- If the value of *port* is 1, the system configures the object with a port number of 0.
- If the value of *port* is in the range of 2 to 65535, the system configures the object with a port number range of $[0, port-1]$.

When you use the **gt port** option, follow these guidelines:

- The value of *port* cannot be 65535.
- If the value of *port* is 65534, the system configures the object with a port number of 65535.
- If the value of *port* is in the range of 0 to 65533, the system configures the object with a port number range of $[port+1, 65535]$.

When you use the **range port1 port2** option, follow these guidelines:

- If *port1* is equal to *port2*, the system configures the object with the port number *port1*.
- If *port1* is smaller than *port2*, the system configures the object with the port number range.
- If *port1* is greater than *port2*, the system changes the range to $[port2, port1]$ and configures the object with the changed port number range.
- If *port1* is 0, the range is displayed as **lt port2+1**.
- If *port2* is 65535, the range is displayed as **gt port1-1**.

Examples

Configure a service object with a protocol number of **100**.

```
<Sysname> system-view
```

```
[Sysname] object-group service servicegroup
```

```
[Sysname-obj-grp-service-servicegroup] service 100
```

Configure a service object with the source and destination port numbers for the TCP service.

```

<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service tcp source eq 100 destination range 10 100
# Configure a service object with the message type and code for the ICMP service.
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service icmp 100 150

```

Modified feature: Applying a QoS policy to an interface

Feature change description

As from this release, you can apply a QoS policy to a Layer 3 aggregate interface or Layer 3 aggregate subinterface.

Command changes

Syntax

```

qos apply [ remarking | tcp-erspan ] policy policy-name { inbound | outbound }
undo qos apply [ remarking | tcp-erspan ] policy policy-name { inbound | outbound }

```

Views

Interface view

Change description

Before modification: You can apply a QoS policy to a Layer 2 Ethernet interface or Layer 3 Ethernet interface.

After modification: You can apply a QoS policy to a Layer 2 Ethernet interface, Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 3 aggregate interface, or Layer 3 aggregate subinterface.

Usage guidelines

When the traffic class matches the VLAN IDs in outer VLAN tags, Layer 3 Ethernet interfaces and Layer 3 Ethernet subinterfaces do not support QoS policies.

Modified feature: Configuring the authentication load sharing mode for users attached to DRNI interfaces

Feature change description

As from this release, the default authentication load sharing mode for users attached to DRNI interfaces changes from distributed local mode to centralized mode.

Command changes

Modified command: port-security drni load-sharing-mode

Syntax

```
port-security drni load-sharing-mode { centralized | distributed
{ even-mac | local | odd-mac } }
undo port-security drni load-sharing-mode
```

Views

System view

Change description

Before modification: The default authentication load sharing mode for users attached to DRNI interfaces is distributed local.

After modification: The default authentication load sharing mode for users attached to DRNI interfaces is centralized.

Modified feature: Setting the maximum number of configuration archives for local archiving

Feature change description

As from this version, the value range for the maximum number of configuration archives that can be saved on the device changes from 1 to 10 to 1 to 1000.

Command changes

Modified command: archive configuration max

Syntax

```
archive configuration max file-number
```

Views

System view

Change description

Before modification: The value range for the *file-number* argument is 1 to 10.

After modification: The value range for the *file-number* argument is 1 to 1000.

Modified feature: Displaying detailed next hop information in the RIB or for direct routes or static routes

Feature change description

As from this version, the **Age**, **ExtFlag**, and **Flags** fields were added to the commands used to display detailed next hop information in the RIB or for direct routes or static routes.

- The **Age** field displays the elapsed time since a next hop was last updated.
- The **ExtFlag** field displays the extended flag of a next hop.
- The **Flags** field displays the flags of a next hop.

Command changes

Modified command: display rib nib

Use **display rib nib** to display next hop information in the RIB.

Syntax

```
display rib nib [ self-originated ] [ nib-id ] [ verbose ]
display rib nib protocol protocol [ verbose ]
```

Views

Any view

Change description

Before modification: The detailed next hop information in the RIB does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information in the RIB contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

Modified command: display route-direct nib

Use **display route-direct nib** to display next hop information for direct routes.

Syntax

```
display route-direct nib [ nib-id ] [ verbose ]
```

Views

Any view

Change description

Before modification: The detailed next hop information for direct routes does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information for direct routes contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.

- The flags of a next hop.

Modified command: display ipv6 rib nib

Use **display ipv6 rib nib** to display next hop information in the IPv6 RIB.

Syntax

```
display ipv6 rib nib [ self-originated ] [ nib-id ] [ verbose ]
display ipv6 rib nib protocol protocol [ verbose ]
```

Views

Any view

Change description

Before modification: The detailed next hop information in the IPv6 RIB does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information in the IPv6 RIB contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

Modified command: display ipv6 route-direct nib

Use **display ipv6 route-direct nib** to display next hop information for IPv6 direct routes.

Syntax

```
display ipv6 route-direct nib [ nib-id ] [ verbose ]
```

Views

Any view

Change description

Before modification: The detailed next hop information for IPv6 direct routes does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information for IPv6 direct routes contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

Modified command: display route-static nib

Use **display route-static nib** to display next hop information for static routes.

Syntax

display route-static nib [*nib-id*] [**verbose**]

Views

Any view

Change description

Before modification: The detailed next hop information for static routes does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information for static routes contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

Modified command: display ipv6 route-static nib

Use **display ipv6 route-static nib** to display next hop information for IPv6 static routes.

Syntax

display ipv6 route-static nib [*nib-id*] [**verbose**]

Views

Any view

Change description

Before modification: The detailed next hop information for IPv6 static routes does not contain the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

After modification: The detailed next hop information for IPv6 static routes contains the **Age**, **ExtFlag**, and **Flags** fields to display the following information:

- The elapsed time since a next hop was last updated.
- The extended flag of a next hop.
- The flags of a next hop.

Modified feature: Optimizing BMP server information display

Feature change description

As from this release, the **Statistics report interval**, **Reported route mode**, **Pu-monitor-mode**, and **Pd-monitor-mode** fields are added to the output of the **display bgp bmp server** command.

Command changes

Modified command: display bgp bmp server

Examples

```
# Display information about BMP server 1.
<Sysname> display bgp bmp server 1
BMP server number: 1
Server VPN instance name: vpna
Server address: 100.1.1.1  Server port: 6895
Client address: 100.1.1.2  Client port: 21452
BMP server state: Connected  Up for 00h41m53s
TCP source interface has been configured
Statistics report interval: 5s
Reported route mode: adj-rib-in pre-policy
Pu-monitor-mode: Enabled
Pd-monitor-mode: Enabled

Message statistics:
Total messages sent: 15
    INITIATION: 1
    TERMINATION: 0
    STATS-REPORT: 0
    PEER-UP: 4
    PEER-DOWN: 3
    ROUTE-MON: 7

BGP peers monitored by BMP server:
    10.1.1.1
```

Change description

As from this release, the following fields are added to the output of this command:

- **Statistics report interval**—Interval at which BGP sends statistics information to the BMP server.
- **Reported route mode**—Type of the routes that BGP reports to the BMP server.
- **Pu-monitor-mode**—Whether the BMP client sends peer up notifications with mode flags to the BMP server.
- **Pd-monitor-mode**—Whether the BMP client sends peer down notifications with mode flags to the BMP server.

Modified feature: Setting the 802.1X periodic reauthentication timer

Feature change description

As from this version, the value range for the 802.1X periodic reauthentication timer set in system view and interface view was changed from 60 to 7200 seconds to 60 to 86400 seconds.

Command changes

Modified command: dot1x timer reauth-period (interface view)

Syntax

```
dot1x timer reauth-period reauth-period-value  
undo dot1x timer reauth-period
```

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Change description

Before modification: The value range for the *reauth-period-value* argument is 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified command: dot1x timer

Syntax

```
dot1x timer { ead-timeout ead-timeout-value | handshake-period handshake-period-value | quiet-period quiet-period-value | reauth-period reauth-period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-value | tx-period tx-period-value | unicast-trigger unicast-trigger-value | quiet-period quiet-period-value | user-aging { auth-fail-vlan | auth-fail-vsi | critical-microsegment | critical-vlan | critical-vsi | guest-vlan | guest-vsi } aging-time-value }  
undo dot1x timer { ead-timeout | handshake-period | quiet-period | reauth-period | server-timeout | supp-timeout | tx-period | unicast-trigger | quiet-period | user-aging { auth-fail-vlan | auth-fail-vsi | critical-microsegment | critical-vlan | critical-vsi | guest-vlan | guest-vsi } }
```

Views

System view

Change description

Before modification: The value range for the *reauth-period-value* argument is 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified feature: Setting the periodic MAC reauthentication timer

Feature change description

As from this version, the value range for the periodic MAC reauthentication timer set in system view and interface view was changed from 60 to 7200 seconds to 60 to 86400 seconds.

Command changes

Modified command: mac-authentication timer (interface view)

Syntax

```
mac-authentication timer { auth-delay auth-delay-time | reauth-period reauth-period-value }  
undo mac-authentication timer { auth-delay | reauth-period }
```

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Change description

Before modification: The value range for the *reauth-period-value* argument is 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified command: mac-authentication timer (system view)

Syntax

```
mac-authentication timer { offline-detect offline-detect-value | quiet quiet-value | reauth-period reauth-period-value | server-timeout server-timeout-value | temporary-user-aging aging-time-value | user-aging { critical-microsegment | critical-vlan | critical-vsi | guest-vlan | guest-vsi } aging-time-value }  
undo mac-authentication timer { offline-detect | quiet | reauth-period | server-timeout | temporary-user-aging | user-aging { critical-microsegment | critical-vlan | critical-vsi | guest-vlan | guest-vsi } }
```

Views

System view

Change description

Before modification: The value range for the *reauth-period-value* argument is 60 to 7200 seconds.

After modification: The value range for the *reauth-period-value* argument is 60 to 86400 seconds.

Modified feature: Displaying local public keys

Feature change description

The **Key length** field was added to the output for the **display public-key local public** command to indicate the key length of public keys in local key pairs, in bits.

Command changes

Modified command: display public-key local public

Syntax

```
display public-key local { dsa | ecdsa | rsa } public [ name key-name ]
```

Views

Any view

Change description

The **Key length** field was added to the output for this command to indicate the key length of public keys in local key pairs, in bits.

Modified feature: Value range for the ID of an IPsec tunnel

Feature change description

The value range for the *tunnel-id* argument changed.

Command changes

Modified command: display ipsec statistics

Syntax

```
display ipsec statistics [ tunnel-id tunnel-id ]
```

Views

Any view

Change description

Before modification, the value range for the *tunnel-id* argument was 0 to 4294967295.

After modification, the value range for the *tunnel-id* argument is 0 to 4294967294.

Modified command: display ipsec tunnel

Syntax

```
display ipsec tunnel { brief | count | tunnel-id tunnel-id }
```

Views

Any view

Change description

Before modification, the value range for the *tunnel-id* argument was 0 to 4294967295.

After modification, the value range for the *tunnel-id* argument is 0 to 4294967294.

Modified command: reset ipsec statistics

Syntax

```
reset ipsec statistics [ tunnel-id tunnel-id ]
```

Views

Any view

Change description

Before modification, the value range for the *tunnel-id* argument was 0 to 4294967295.

After modification, the value range for the *tunnel-id* argument is 0 to 4294967294.

Modified feature: Configuring automatic email sending parameters for an EAA monitor policy

Feature change description

As from this release, the length of the email server domain name is changed to 1 to 253 characters.

Command changes

Modified command: rtm email domain

Syntax

```
rtm email domain domain-name
```

Views

System view

Change description

Before modification: The *domain-name* argument is a string of 1 to 255 characters.

After modification: The *domain-name* argument is a string of 1 to 253 characters.

Modified feature: Setting the usage alarm threshold of a log file

Feature change description

The value range for the usage alarm threshold of a log file was changed to 0 to 100, in percentage.

Command changes

Modified command: info-center logfile alarm-threshold

Syntax

```
info-center logfile alarm-threshold usage
```

Views

System view

Change description

Before modification, the value range for the usage alarm threshold of a log file was 1 to 100, in percentage.

After modification, the value range for the usage alarm threshold of a log file is 0 to 100, in percentage.

Modified feature: Displaying heap memory usage for a user process

Feature change description

As from this version, the **Free physical memory ratio** field is added to the output from the command that displays the heap memory usage for a user process.

Command changes

Modified command: display process memory heap

Syntax

```
display process memory heap job job-id [ verbose ] [ slot slot-number [ cpu cpu-number ] ]
```

Views

Any view

Change description

Before modification: The command does not support displaying the **Free physical memory ratio** field in the output.

After modification: The command supports displaying the **Free physical memory ratio** field in the output.

Modified feature: Displaying gRPC information

Feature change description

As from this release, the device supports displaying both detailed and brief information about both gRPC dial-in mode and gRPC dial-out mode. With previous releases, the device can display only brief gRPC dial-in mode information.

Command changes

Old syntax

display grpc

New syntax

display grpc [verbose]

Views

Any view

Change description

Before modification: The device supports displaying only brief information about only gRPC dial-in mode.

After modification: The device supports displaying both detailed and brief information about both gRPC dial-in mode and gRPC dial-out mode. To display detailed information, specify the **verbose** keyword. To display brief information, do not specify the **verbose** keyword.

R6615P07

This release has the following changes:

- [Removed feature: Enabling the SSH server to support SSH1 clients](#)
- [Removed feature: Setting the minimum interval for updating the RSA server key pair](#)

Removed feature: Enabling the SSH server to support SSH1 clients

Feature change description

As from this version, this feature is not supported.

Deleted command

ssh server compatible-ssh1x enable

Syntax

```
ssh server compatible-ssh1x enable
undo ssh server compatible-ssh1x [ enable ]
```

Views

System view

Removed feature: Setting the minimum interval for updating the RSA server key pair

Feature change description

As from this version, this feature is not supported.

Deleted command

ssh server rekey-interval

Syntax

```
ssh server rekey-interval interval
undo ssh server rekey-interval
```

Views

System view

.

R6615P06

First release.