Hewlett Packard Enterprise

HPE 5130HI-CMW710-R3507P18-US Release Notes

Contents

List of tables

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 5130HI-CMW710-R3507P18-US. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE 5130HI-CMW710-R3507P18-US Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 3507P18-US

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

Version history

IMPORTANT:

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

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
R3507P18-US	R3507P10	2023-10-27	Release	This version fixed bugs
R3507P10	R3507P09	2023-03-09	Release	This version fixed bugs
R3507P09	R3507P06	2023-02-01	Release	This version fixed bugs
R3507P06	R3507P02	2022-07-01	Release	This version fixed bugs
R3507P02	R3507	2021-12-25	Release	This version fixed bugs
R3507	R3506P11	2021-06-08	Release	This version fixed bugs and introduced feature changes. New features include: • EAD assistant
R3506P11	R3506P10	2021-01-29	Release	This version fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R3506P10	R3506P08	2020-11-13	Release	This version fixed bugs and introduced feature changes. New features include: • Configuring the 802.1p priority for control packets sent by a device • Packet spoofing logging and filtering entry logging for SAVI • Configuring password control over weak passwords • Enabling password change prompt logging • Enabling recording untrusted DHCP servers on a DHCP snooping device There are also modified features.
R3506P08	R3506P06	2020-07-27	Release	This version fixed bugs.
R3506P06	R3506P03	2020-06-19	Release	This version fixed bugs and introduced feature changes. New features include: • Enabling recording untrusted DHCP servers on a DHCP snooping device There are also modified features.
R3506P03	R3506P02	2020-03-24	Release	This version fixed bugs.
R3506P02	R3506P01	2019-12-23	Release	This version fixed bugs.
R3506P01	R3506	2019-10-31	Release	This version fixed bugs.
R3506	R1311P03	2019-07-12	Release	This version fixed bugs and introduced feature changes. New features include: • For more information about the new features, see *HPE 5130HI-CMW710-R3506 Release Notes (Software Feature Changes)* There are also modified features. Fixed bugs
R1311P03	R1311P02	2019-04-01	Release	This version fixed bugs and introduced feature changes. New features include: • Using USB-based automatic configuration • Setting the block timer for MAC addresses in the blocked MAC address list • Logging off 802.1X users • Logging off MAC authentication users Fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R1311P02	R1311P01	2019-02-20	Release version	This version fixed bugs.
R1311P01	R1309P07	2018-12-26	Release version	This version fixed bugs and introduced feature changes. New features include: • Specifying DNS server information in RA messages • Specifying DNS suffix information in RA messages • Suppressing advertising DNS information in RA messages • HTTP redirect There are also modified features. Fixed bugs
R1309P07	R1309P06	2018-09-26	Release version	This version fixed bugs and introduced feature changes. New features include: • Automatic obtaining of the login username for temporary user role authorization • 802.1X EAP-TLS fragmentation for packets sent to the server There are also modified features. Fixed bugs
R1309P06	R1309P03	2018-08-02	Release version	This version fixed bugs and introduced feature changes. New features include: • Enabling interface consistency check for ARP and MAC address entries • 802.1X offline detection There are also modified features. Fixed bugs
R1309P03	R1309	2018-04-27	Release version	This version fixed bugs and introduced feature changes. New features include: • PD detection mode • 802.1X user logging • MAC authentication user logging • Port security user logging • Configuring the Event MIB Removed feature: • Enabling PoE for a PSE

Version number	Last version	Release Date	Release type	Remarks
R1309	R1308	2017-08-15	Release version	This version fixed bugs and introduced feature changes. New features include: • MAC address information display for 802.1X users in 802.1X VLANs of a specific type • Authorization CAR action in an ISP domain • 802.1X client There are also modified features.
R1308	R1121P03	2017-03-07	Release version	This version introduced feature changes. New features include: • Fundamentals features • IRF features • Layer 2-LAN switching features Removed features: • CFD: Hardware CC There are also modified features. See the *Software Feature Changes* document for this release notes.
R1121P03	R1121P02	2016-12-22	Release version	New feature: • Link aggregation management VLANs and management port • ISP domain for users assigned to nonexistent domains Modified feature: • Maximum length of jumbo frames allowed by an Ethernet interface • Username format modification for device login Fixed bugs
R1121P02	R1121	2016-11-25	Release version	Modified feature: • SSH listening port Fixed bugs
R1121	R1120P10	2016-07-11	Release version	Modified feature: • Specifying log hosts Fixed bugs

Version number	Last version	Release Date	Release type	Remarks
R1120P10	R1120P07	2016-07-11	Release version	New feature: • 802.1X critical voice VLAN • MAC authentication critical voice VLAN • MAC authentication support for Session-Timeout and Termination-Action attributes • Enabling SNMP notifications for port security Modified feature: • CDP enhancement • Configuring a test profile for RADIUS server status detection • NTP support for ACL • Storm control for known unicast packets Fixed bugs
R1120P07	R1120P05	2016-05-19	Release version	New features Modified features • Display Mac address entries Fixed bugs
R1120P05	R1120	2016-04-01	Release version	• New features • Modified features Fixed bugs
R1120	R1118P02	2016-03-13	Release version	New feature: • Specifying ITU channel numbers for transceiver modules • ISSU • Configuring the DHCP smart relay feature • RADIUS server status detection • RADIUS server load sharing • Sending EAP-Success packets to 802.1X users in critical VLAN • ND Snooping • ND attack detection • RA guard • Setting port security's limit on the number of secure MAC addresses for specific VLANs Modified feature: • Maximum number of secure MAC addresses on a port for port security • Specifying RADIUS servers Fixed bugs

Version number	Last version	Release Date	Release type	Remarks
R1118P02	R1118	2015-12-30	Release version	New feature: • MACsec Fixed bugs
R1118	R1111P01	2015-12-08	Release version	New feature: • Disable SSL session renegotiation for the SSL server • IPsec support for Suite B • SSH support for Suite B • Public key management support for Suite B • PKI support for Suite B • SSL support for Suite B Modified feature: • FIPS self-tests Fixed bugs
R1111P01	First release	2015-10-13	Release version	First release

Hardware and software compatibility matrix

CAUTION:
To avoid an upgrade failure, use Table 2 verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	5130HI Series
Hardware platform	HPE 5130 24G 4SFP+ 1-slot HI Switch JH323A HPE 5130 48G 4SFP+ 1-slot HI Switch JH324A HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A HPE 5130 48G PoE+ 4SFP+ 1-slot HI Switch JH326A
Minimum memory requirements	2 GB
Minimum Flash requirements	512 M
Boot ROM version	Version 128 or higher (Note: Use the **display version** command in any view to view the version information. Please see **Note②**)

Item	Specifications
Host software & SHA 256 Checksum	5130HI-CMW710-R3507P18-US.ipe 18DBD63A3656AC269F9FC92D039CF7EF9BDB23CB6CC370D8A6A35484BF506E1E 5130hi-cmw710-freeradius-r3507p18-US.bin EB87F6663D0DD07273EAEECE992E9F70C2A636BBD3F9EE0EBF71388732DEB500 5130hi-cmw710-packet-capture-r3507p18-US.bin 2D88ED9D2EBFE55D442F1EAF60BA2AC6ABD2297F81C95B63D04817504D291115
iMC version	iMC BIMS 7.3(E0506H01) iMC EAD 7.3(E0611P10) iMC QoSM 7.3(E0505P01) iMC EIA 7.3(E0611P13) iMC PLAT 7.3(E0705P12) iMC NTA 7.3(E0707L06) iMC SHM 7.3(E0707L06)
iNode version	iNode PC 7.3(E0585)
Web version	None
Remarks	None

Display the system software and Boot ROM versions of 5130HI:

```
<HPE>display version
HPE Comware Software, Version 7.1.070, Release 3507P10       ------ Note①
Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP
HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A uptime is 0 weeks, 0 days, 0 hours, 8 minutes
Last reboot reason : User reboot

Boot image: flash:/5130hi-cmw710-boot-r3507p10.bin
Boot image version: 7.1.070, Release 3507P10
  Compiled Oct 17 2021 11:00:00
System image: flash:/5130hi-cmw710-system-r3507p10.bin
System image version: 7.1.070, Release 3507P10
  Compiled Oct 17 2021 11:00:00


Slot 1:
Uptime is 0 weeks,0 days,0 hours,8 minutes
5130 24G PoE+ 4SFP+ 1-slot HI Switch with 2 Processor
BOARD TYPE:          5130 24G PoE+ 4SFP+ 1-slot HI Switch
DRAM:                1984M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.B
Bootrom Version:     128             ------ Note②
CPLD 1 Version:      003
Release Version:     HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A-3507P10
Patch Version  :     None
Reboot Cause   :     UserReboot
```

```
[SubSlot 0] 24GE+4SFP Plus
```

ISSU upgrade type matrix

ISSU provides two upgrade types: compatible upgrade and incompatible upgrade. 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 is performed.

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

Table 3 ISSU version compatibility matrix

Current version	History version	ISSU upgrade method
5130HI-CMW710-R3507P18-US	5130HI-CMW710-R3507P10	Compatible
	5130HI-CMW710-R3507P09	Compatible
	5130HI-CMW710-R3507P06	Compatible
	5130HI-CMW710-R3507P02	Compatible
	5130HI-CMW710-R3507	Compatible
	5130HI-CMW710-R3506P11	Compatible
	5130HI-CMW710-R3506P10	Compatible

Upgrade advice

Upgrade to this version is mandatory.

Upgrade restrictions and guidelines

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

Hardware feature updates

Hardware feature updates in R3507P18-US~3506P02

None

Hardware feature updates in R3506P01

Added support for the SFP-XG-LH40-SM1270-BIDI, SFP-XG-LX-SM1270-BIDI, SFP-XG-LX-SM1330-BIDI, and SFP-XG-LH40-SM1330-BIDI transceiver modules.

Hardware feature updates in R3506~R1121P02

None

Hardware feature updates in R1121

The data in 错误!未找到引用源。 was modified according to the newest test results.

Hardware feature updates in R1120P10~R1118

None

Hardware feature updates in R1111P01

First release

Software feature and command updates

For more information about the software feature and command update history, see *HPE HI-CMW710-R3507P10 Release Notes (Software Feature Changes).*

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
5130HI-CMW710-R3507P10~5130HI-CMW710-R3506P11			
New	None	None	None
Modified	None	None	None
5130HI-CMW710-R3506P10			
New	savi.mib	SAVI-MIB	Added the following objects to SaviObjectsSystemEntry: saviObjectsSystemNotifySpoofing used for setting or obtaining the status of packet spoofing logging. saviObjectsSystemNotifyFilter used for setting or obtaining the status of filtering entry logging. saviObjectsSystemNotifySpoofingInterval used for setting or obtaining the log output interval for packet spoofing logging. saviObjectsSystemNotifySpoofingNumber used for setting or obtaining the maximum number of log messages that can be output per interval.

Item	MIB file	Module	Description
			saviObjectsSystemBindingCount used for obtaining the number of binding entries. saviObjectsSystemFilteringCount used for obtaining the number of filtering entries. Added the following object to SaviObjectsCountEntry: saviObjectsCountFilterOctets used for obtaining the byte count for spoofed packets filtered by SAVI.
Modified	None	None	None
5130HI-CMW710-R3506P08~5130HI-CMW710-R1118			
New	None	None	None
Modified	None	None	None
5130HI-CMW710-R1111P01			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R3507P18-US

None

Operation changes in R3507P10

None

Operation changes in R3507P09

None

Operation changes in R3507P06

None

Operation changes in R3507P02

None

Operation changes in R3507

- When the number of MAC address entries learned on a port reaches the upper limit, the message generated for this issue has changes.
  - Before modification: The message is `The number of MAC address entries exceeded the maximum number.`
  - After modification: The message is `The number of MAC address entries reached the maximum number.`

Operation changes in R3506P11

- Removed consistency check between the specified and actual airflow directions of the fan trays.
- Excluded the *freeradius.bin* file from the IPE file.

Operation changes in R3506P10

None

Operation changes in R3506P08

None

Operation changes in R3506P06

The following commands were added to the default configuration file:

```
password-control enable
#
local-user admin
service-type terminal
authorization-attribute user-role network-admin
#
user-interface aux 1
authentication-mode scheme
#
undo password-control aging enable
undo password-control composition enable
undo password-control history enable
undo password-control length enable
password-control login idle-time 0
password-control login-attempt 3 exceed unlock
password-control update-interval 0
```

Operation changes in R3506P03

None

Operation changes in R3506P02

None

Operation changes in R3506P01

None

Operation changes in R3506

After you set the speed to 100 Mbps and the duplex mode to full on an interface installed with a GE transceiver module, the interface can work with an interface with a 100MB transceiver module installed.

Modified the 802.1p priority in the VLAN tags of ARP replies sent by the device from 0 to 6

Operation changes in R1311P03

None

Operation changes in R1311P02

None

Operation changes in R1311P01

Providing RPS failure log messages

The device outputs the RPS Failed log message when you remove an RPS DC power cable.

Operation changes in R1309P07

None

Operation changes in R1309P06

None

Operation changes in R1309P03

- Changed the ACL issuing operation

  Before modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on client MAC addresses.

  After modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on CLASS-IDs rather than client MAC addresses. The device uses the same CLASS-ID when issuing Layer 2 ACLs to authentication users with the same authorization ACL, which saves ACL resources.

Operation changes in R1309

None

Operation changes in R1308

Before the modification: A PoE switch enabled with LLDP does not perform any operations if it has not received any LLDP frames from a connected AP before the defined timer expires.

After the modification: A PoE switch enabled with LLDP power cycles the PoE port (PI) and reboots a connected AP forcibly if it has not received any LLDP frames from the AP before the defined timer expires.

Operation changes in R1121P03

None

Operation changes in R1121P02

None

Operation changes in R1121

None

Operation changes in R1120P10

None

Operation changes in R1120P07

None

Operation changes in R1120P05

None

Operation changes in R1120

None

Operation changes in R1118P02

None

Operation changes in R1118

None

Operation changes in R1111P01

First release

Restrictions and cautions

Restrictions

Hardware

The following transceiver modules can only work in the SFP+ ports of an HPE 5130/5510 10GbE SFP+ 2-port module (JH157A). Do not install the transceiver module in an SPF+ port on the front panel.

- HPE X130 10G SFP+ LC LRM transceiver modules (JD093B)
- HPE X130 10G SFP+ LC LH 80km Transceiver (JG915A)
- HPE X130 10G SFP+ LC ER 40km Transceiver (JG234A)

Software

When you configure 802.1X authentication and MAC authentication, follow these restrictions:

a. When users with ACLs assigned exist on a single port, you must assign ACLs (for example, ACLs with the permit rule) to the users that do not need ACLs assigned. This operation ensures that these users do not mistakenly match ACLs of other users.

b. You must adjust the ACL rule positions to ensure that the traffic of each online user can match rules in the ACL assigned to the user.

c. When multiple users come online on a port and the same ACL is assigned to these users, to add rules to or delete rules from the ACL, you must first log off all users on the port and then add or delete ACL rules. Otherwise, some deleted ACL rules will remain.

If you configure both a PBR policy and an inbound QoS policy containing a traffic policing action, only the PBR policy takes effect on the traffic matching both policies.

If you configure both a PBR policy and a QoS policy containing a deny action, only the PBR policy takes effect on the traffic matching both policies.

Cautions

None

Open problems and workarounds

None

List of resolved problems

Resolved problems in R3507P18-US

202307030467

- Symptom: Failed to deploy VLAN configuration from IMC to the switch.
- Condition: This symptom occurs when you create a VLAN and assign the VLAN to all trunk ports and hybrid ports from IMC.

Resolved problems in R3507P10

202303021705

- Symptom: The switch fails to forward PTP packets.
- Condition: This symptom occurs if PIM-DM and IGMP are configured on the switch.

Resolved problems in R3507P09

202209030500

- Symptom: The switch prints a log message that CRC errors packets were received.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable flow sampling and specify the number of packets out of which flow sampling samples a packet in Ethernet interface view.
  b. The packets received on the interface are sent to the CPUs of other IRF member devices through IRF physical links.

202208111206

- Symptom: PIM packets cannot be forwarded at Layer 2.
- Condition: This symptom occurs if IGMP snooping is enabled.

202208100206

- Symptom: The system might prompt insufficient ACL resources.
- Condition: This symptom occurs if a packet filter is applied to an interface and then rules in the ACL of the packet filter are modified.

Resolved problems in R3507P06

202203290188

- Symptom: VLANs that do not belong to an AC interface are blocked.
- Condition: This symptom occurs if STP is enabled on the AC interface in an L2VPN network.

Resolved problems in R3507P02

202107110018

- Symptom: The aggregate interface configured as an MFF network port forwards received ARP requests out of its member interfaces.
- Condition: This symptom occurs if a Layer 2 aggregate interface is configured as an MFF network port after MFF is enabled.

202108250280

- Symptom: Batch backup fails to complete when BGP NSR backs up data from the active BGP process to the standby BGP process consecutively.
- Condition: This symptom might occur when BGP NSR backs up data from the active BGP process to the standby BGP process consecutively.

202107050836

- Symptom: Error logs about unsupported or unavailable transceiver modules are generated repeatedly, resulting in high CPU usage.
- Condition: This symptom occurs if the following conditions exist:
  - The device is installed with an incompatible transceiver module or not installed with any transceiver modules.
  - Network management software retrieves information about transceiver modules periodically.

202107211304

- Symptom: Failed to save the running configuration.
- Condition: This symptom might occur when you use the **`save`** command to save the running configuration.

202107191057

- Symptom: Some 802.1X users cannot come online on a port.
- Condition: This symptom might occur if the following conditions exist:
  - The port is enabled with both 802.1X authentication and MAC authentication.
  - A large number of users are repeatedly coming online and going offline.

202107211171

- Symptom: After you execute the **silent-interface all** command for the OSPF process, execute the **`undo silent-interface`** command for the OSPF interface, and restart the device, the configuration of the **undo silent-interface** command does not take effect, causing OSPF neighbor relationship establishment failures.
- Condition: This symptom might occur when you execute the **silent-interface all** command for the OSPF process, execute the **`undo silent-interface`** command for the OSPF interface, and then restart the device.

202107220559

- Symptom: BGP peer flapping with a packet loss duration of nine seconds occurs after an active/standby switchover, and error message **Send notification with error 5/0** is displayed.
- Condition: This symptom might occur when the following conditions exist:
  - An active/standby switchover occurs on the device.
  - The configuration on the BGP peer of the device changes during the switchover and the peer sends Refresh packets to the device.

202107110017

- Symptom: The aggregate interface sends a received ARP reply out of a member interface back to the upstream device, and the upstream device reports a MAC move event.
- Condition: This symptom occurs after the **arp detection trust** command is executed on an aggregate interface and the aggregate interface receives an ARP reply.

202108230830

- Symptom: The device falsely reports CRC error packet notifications for IRF ports.
- Condition: This symptom might occur if the device has been running for a period of time and a number of ports are forwarding traffic.

202109240201

- Symptom: All devices are elected as the master in the IPv6 VRRP group, and they cannot ping each another.
- Condition: This symptom occurs if you configure the **mld-snooping source-deny** command for a member port in a dynamic aggregation group.

202109240467

- Symptom: The system prompts that a QoS policy failed to be applied to an interface, and flow mirroring ERSPAN failed.
- Condition: This symptom occurs if you configure flow mirroring ERSPAN for an aggregation group member port and the aggregation group member port comes up and goes down multiple times.

202107160918

- Symptom: The lldp process might exit unexpectedly.
- Condition: This symptom might occur if aggregation groups exist on the device and the lldpLocManAddrEntry table in the MIB is regularly accessed.

202107191086

- Symptom: After some 802.1X users come online, no authorization VLAN or VSI is assigned to them.
- Condition: This symptom occurs if the following operations are performed:
  a. Both 802.1X authentication and MAC authentication are enabled on interface.
  b. ACLs are assigned to MAC authentication users.
  c. Users come online and then go offline.
  d. VLANs or VSIs are assigned to 802.1X users.

202103311306

- Symptom: Failed to delete a permanent static route.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure a permanent static route and specify a preference lower than common static routes for the permanent static route.
  b. Change the output interface address of the permanent static route and change the permanent static route settings multiple times. The permanent static route is recursed to a common route or to Null 0.
  c. Delete the permanent static route.

Resolved problems in R3507

202105110200

- Symptom: An incorrect neighbor management address is displayed in the output from the **display lldp neighbor-information verbose** command.
- Condition: This symptom occurs if the following conditions exist:
  - The length of the value in the Management Address TLV is less than 8 bytes in the CDP packets received by the device.
  - The total length of the Management Address TLV is less than 12 bytes.

202104220726

- Symptom: User credential information leaks.
- Condition: This symptom might occur when the user logs in to the Web interface of the device.

202105211293

- Symptom: When the SNMP NMS reads the temperature sensor MIB node, an alarm is generated abnormally.
- Condition: This symptom occurs if the device does not have an OAP security subcard inserted.

202105060531

- Symptom: Host routes become invalid on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the host routes have different next hops.

202105110235

- Symptom: The number of secure MAC addresses on a port has reached the upper limit. However, port security does not work as expected when a user moves from another port to this port.
- Condition: This symptom occurs if the following operations are performed:
  a. Port security is enabled on both of the ports. On each of the ports, the MAC address of a user is configured as a secure MAC address. The secure MAC addresses configured on the two ports are different.
  b. The two ports learn MAC addresses from each other.
  c. The users that use the configured secure MAC addresses move between the two ports.

202103290727

- Symptom: The netmeisterd process runs abnormally on an IRF fabric.
- Condition: This symptom occurs if third-party network management software cannot correctly recognize the H3C IRF fabric and issues a command to reboot the master device of the IRF fabric.

202102230116

- Symptom: The DHCP address pool fails to assign IP addresses to clients from its second secondary subnet.
- Condition: This symptom might occur if no IP addresses are available for dynamic allocation on the primary subnet and first secondary subnet in the DHCP address pool.

202104200379

- Symptom: The device reboots unexpectedly after running for a period of time.
- Condition: This symptom occurs if the device receives IP packets destined to 239.255.255.250 and with the TTL as 1 or 2.

202102150008

- Symptom: The **netconf log source all verbose** command gets stuck on an IRF fabric with an extremely low probability.
- Condition: This symptom might occur after a master/subordinate switchover if the IRF fabric is configured with loop detection and AAA or NETCONF services exist on the IRF fabric.

202103241845

- Symptom: After you modify the device IP, the device can still access the network.
- Condition: This symptom occurs if the actual number of ARP snooping entries on the device is different from that collected by the counter.

202102160026/202102221454

- Symptom: Online MAC authentication users are logged out on an IRF fabric because their idle timeout timer expires. However, the users are continuously sending traffic to the device.
- Condition: This symptom occurs if a master/subordinate switchover has occurred on the IRF fabric.

202102100037

- Symptom: A number of MAC authentication users are logged out on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the online duration of these MAC authentication users is longer than the session timeout period assigned by the server after the master/subordinate switchover.

202104200312

- Symptom: MAC authentication users cannot come online on a port.
- Condition: This symptom might occur if the MAC authentication users come online and go offline repeatedly on the port when the following conditions exist:
  - The port is enabled with both 802.1X authentication and MAC authentication.
  - The port is configured with the 802.1X guest VLAN.

Resolved problems in R3506P11

202101190167

- Symptom: After ARP fast update is enabled for MAC address moves, IPv6 ND entries are not fast updated when MAC addresses move.
- Condition: This symptom might occur after the **`mac-address mac-move fast-update`** command is executed.

202101190137

- Symptom: The device reboots automatically with a low probability when it runs the R3506P08 or R3506P10 software version. The reboot reason is reported as **UserReboot**.
- Condition: This symptom might occur when the device runs the R3506P08 or R3506P10 software version.

Resolved problems in R3506P10

202010120344

- Symptom: An IRF master device hangs and cannot be accessed through the console port.

- Condition: This symptom might occur if an IRF fabric receives packets shorter than 64 bytes.

202009220628

- Symptom: The device cannot identify phone offline events.
- Condition: This symptom might occur if the device is attached to phones that do not send CDP packets periodically, such as Polycom and AudioCodes phones.

202009280287

- Symptom: CVE-2020-10188
- Condition: 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.

202008240782

- Symptom: The Telnet process hangs.
- Condition: This symptom might occur if command accounting is enabled and the AAA server is unreachable.

202008240177

- Symptom: Users fail their first portal authentication attempts while passing the second one.
- Condition: This symptom might occur if both the **portal apply mac-trigger-server** and **portal apply web-server settings** are configured.

Resolved problems in R3506P08

202007271063

- Symptom: The device might fail to start properly with a very low probability.
- Condition: This symptom occurs if the device is repeatedly power-cycled.

Resolved problems in R3506P06

202005271313

- Symptom: 1-Gbps fiber ports do not come up.
- Condition: This symptom occurs because 1-Gbps fiber ports cannot be connected to SGMII devices.

202005291034

- Symptom: An aggregate interface does not load share TCP or UDP traffic among member links.
- Condition: This symptom might occur if TCP or UDP traffic is forwarded out of an aggregate interface.

202004020936

- Symptom: Clock synchronization fails after an ISSU is performed.
- Condition: This symptom occurs if you use **the ntp-service source** command to specify a source interface for NTP messages before performing the ISSU.

202005111273

- Symptom: The combo ports on all IRF subordinate devices go down after a master/subordinate switchover.

- Condition: This symptom occurs if the master/subordinate switchover occurs after the original master device reboots or the entire IRF fabric reboots.

Resolved problems in R3506P03

202001170358

- Symptom: 802.1X users and MAC authentication users come online through the same port. The ACL issued to users that come online later does not take effect.
- Condition: This symptom occurs if the following operations have been performed:
  a. Configure both MAC authentication and 802.1X authentication on a port.
  b. Issue the same ACL to users.

Resolved problems in R3506P02

201912170108

- Symptom: When the PoED process is restarted, the process does not respond.
- Condition: This symptom occurs if the following conditions exist:
  - Multiple PoE-capable devices form an IRF fabric.
  - The master and subordinate member devices all act as PSEs to supply power.
  - The PoED process is restarted every 20 seconds.

201911070588

- Symptom: The SSHD call stack might be printed.
- Condition: This symptom occurs if you log in to the device repeatedly through SSH.

201908270157

- Symptom: After a user passes 802.1X authentication and enters the username and password on a PC, ErrCode=0 appears on the switch and the user goes offline. About half a minute to one minute later, the user performs authentication again and comes online.
- Condition: This symptom occurs if the following operations are performed:
  - On an interface configured with port-based access control, configure the guest VLAN and the hybrid port is removed from the default VLAN (VLAN 1).
  - After a user passes 802.1X authentication, the user modifies the username and password and initiates authentication again.

Resolved problems in R3506P01

201909250124

- Symptom: Some interfaces on the device go down.
- Condition: This symptom occurs if the copper ports of the device are configured to autonegotiate their speeds and are connected to APs.

201908270091

- Symptom: After an IRF physical interface is switched to a common interface, multicast traffic is forwarded abnormally on the interface.
- Condition: This symptom occurs if an IRF physical interface is switched to a common interface after IP multicast forwarding is enabled.

Resolved problems in R3506

201904220057

- Symptom: The device tries to obtain the manufacturing information of a fan tray repeatedly, resulting in memory leak.
- Condition: This symptom occurs when no manufacturing information is coded into the fan tray.

201906200052

- Symptom: The port security, LLDP, and interface management processes become deadlocked.
- Condition: This symptom occurs with a low probability if port security is configured on the device and an intrusion protection is triggered.

201906110727

- Symptom: Each time the device is automatically configured after startup, the IP address that it obtains through DHCP is different from the most recent one.
- Condition: This symptom might occur if the configuration on the device is deleted before it reboots and the device is automatically configured after startup.

201906050407

- Symptom: When many-to-one VLAN mapping is configured on the device, a connected terminal cannot ping the extranet after it re-obtains an IP address.
- Condition: This symptom might occur if the terminal re-obtains the IP address after the port through which the terminal connects to the device is moved from an original VLAN to the translated VLAN.

201904200142

- Symptom: On an MPLS L3VPN network, the next hop of the route to the public tunnel is unreachable.
- Condition: This symptom might occur if the device acts as a PE device and the next hop of the route to the public tunnel is equal cost routes but load sharing is not used.

201904160395

- Symptom: The device fails to learn MAC address entries.
- Condition: This symptom might occur if the device has already learned a large number of MAC address entries and multiple ports keep flapping.

201904150324

- Symptom: When the device is configured to display log buffer information and buffered logs, it displays only the newest log rather than all logs in the log buffer.
- Condition: This symptom might occur if the display operation is repeatedly performed after the log buffer gets full.

201904101024

- Symptom: An IRF fabric is split unexpectedly and it cannot process protocol packets correctly.
- Condition: This symptom might occur if an IRF physical interface or a 10-GE port that resides on the same interface module as the IRF physical interface receives a packet with less than 64 bytes.

201904100097

- Symptom: CFD loopback does not take effect on a service instance.
- Condition: This symptom might occur if the MAs in the service instance are configured without carrying the VLAN attribute.

201903290697

- Symptom: Traffic on the main interface of a Layer 3 Ethernet subinterface cannot be forwarded correctly after the subinterface is shut down.
- Condition: This symptom might occur if the Layer 3 Ethernet subinterface is shut down by using the **shutdown** command.

201903280212

- Symptom: Traffic on Layer 3 aggregate subinterfaces in an IRF fabric cannot be forwarded correctly after the IRF fabric reboots.
- Condition: This symptom might occur if the running configuration is saved and the IRF fabric is rebooted after Layer 3 aggregate subinterfaces are configured.

201902020370

- Symptom: Only eight ports on the PoE-capable device can supply power.
- Condition: This symptom might occur if an exception exists on the power management configuration register.

201905140328

- Symptom: When port security is configured, traffic forwarding fails because of secure MAC address loss after the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.
- Conditions: This symptom might occur if the IRF fabric contains three or more member devices and the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.

Resolved problems in R1311P03

201902010586

- Symptom: CVE-2018-5407
- Condition: OpenSSL is prone to a local information-disclosure vulnerability. Local attackers can exploit this issue to obtain sensitive information. This may aid in further attacks.

201812070828

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

201812280425

- Symptom: Multiple Telnet users remain and cannot be deleted, and the CPU usage keeps higher than 50% as a result.
- Condition: This symptom might occur if the Telnet window is closed when a Telnet user logs in to a comsh user and then logs in to a Telnet user.

201812280404

- Symptom: The sshd process deadlock occurs.
- Condition: This symptom might occur if SSH logout is performed when the CPU usage is high.

201812250322

- Symptom: The **arp restricted-forwarding enable** command might not take effect.
- Condition: This symptom occurs if the **arp restricted-forwarding enable** command is configured on the device and the device uses IPSG bindings for forwarding preferentially.

201807260566

- Symptom: In an ADCampus network, an automatically created aggregation group is deleted.
- Condition: This symptom occurs if only one of the aggregation group member ports is up.

201902020416

- Symptom: When the device acts as a BGP BMP client, the device might reboot because the memory is exhausted.
- Condition: This symptom occurs if the following conditions exist:
  - The device has BMP enabled, and establishes a connection to the BMP server through the management interface.
  - The BMP client sends too many data, exceeding the processing capability of the BMP server. As a result, the BMP client actively closes the connection.

Resolved problems in R1311P02

201901210259

- Symptom: The PBR feature does not take effect.
- Condition: This symptom occurs if PBR is configured on a Layer 3 aggregate interface.

Resolved problems in R1311P01

201812060189

- Symptom: A user cannot log in to the switch through SSH when the number of online SSH users reaches 32.
- Condition: This symptom occurs if the device does not update the number of online SSH users after the SSH client logs out.

201812060193

- Symptom: The xmlcfgd process exits unexpectedly and a core file is created.
- Condition: This symptom occurs if the following operations have been performed:
  a. Bind more than 13 static addresses to the DHCP address pool.
  b. Use the SoapUI tool to perform a GET operation on the DHCP/DHCPServerPoolStatic table.

201812060181

- Symptom: The switch reboots unexpectedly after IPsec is configured.
- Condition: This symptom occurs if IPsec is configured.

201812060220

- Symptom: A packet is discarded because it is incorrectly determined as an MPLS ping packet.
- Condition: This symptom occurs if the packet is a UDP fragment and the content after the IP header is the same as the UDP port number (3053).

201811130200

- Symptom: The port security process is locked.
- Condition: This symptom occurs if the following conditions exist:
  - The intrusion protection mode is disableport-temporarily on a port.
  - Port security triggers intrusion protection and sets the port to the down state while LLDP is obtaining user data from port security.

201811050088

- Symptom: The device is connected to an IMC server for portal authentication. The device is logged out because of security check failures.
- Condition: This symptom occurs if the device is connected to an IMC server and IMC is configured with a security policy to perform security check for the device.

201811140403

- Symptom: CVE-2018-15473
- Condition: OpenSSH is prone to a user-enumeration vulnerability. An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks. OpenSSH through 7.7 are vulnerable; other versions may also be affected.

201811300199

- Symptom: A portal user fails re-DHCP authentication, with a "Nonexistent username" error message prompted.
- Condition: This symptom might occur when a portal user performs re-DHCP authentication.

201811050128

- Symptom: Memory leaks occur to the service using the fast forwarding table.
- Condition: This symptom occurs if the following conditions exist:
  a. A large amount of traffic with varying quintuples is sent to the CPU through fast forwarding.
  b. The fast forwarding entries age out.

201811050119

- Symptom: Two devices use IKEv2 negotiation to set up IPsec SAs, and use the security protocol ESP. After TFC padding is enabled, the length of the padded packets exceeds the MTU of the local interface. As a result, packets are dropped.
- Condition: This symptom occurs if the following conditions exist:
  a. The **tfc enable** command is used to enable TFC padding on the peer device.
  b. The length of the padded packets (the original packet length + the TFC padding length) exceeds the MTU of the local interface. Packet fragmentation is disabled.

201811050107

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if the VPN instance and IP address configuration of a 40-GE interface are modified when the interface is sending or receiving packets.

201810230544

- Symptom: The RADIUS server fails to authorize a VLAN name to a user.
- Condition: This symptom occurs if the RADIUS server authorizes a VLAN name in the format of \000XXXXX\000 to a user passing AAA authentication.

201810230551

- Symptom: The memory of the standby MPU leaks.
- Condition: This symptom occurs if a portal client comes online carrying the option82 (v4) or option18 (v6) information on an IRF fabric.

201811010430

- Symptom: The **dot1x offline-detect** and **dot1x offline-detect enable** commands executed on the device do not take effect.
- Condition: This symptom occurs if the software of the device is upgraded to the current version by using ISSU.

201810180032

- Symptom: When you enable BFD on an aggregate interface, the system prompts that the operation failed.
- Condition: This symptom occurs if the low bits of the source IP address and destination IP address are multicast addresses when you enable BFD on an aggregate interface.

201809050571

- Symptom: The controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued. When the display process command is executed, the output shows that a large number of residual configuration copy processes exist on the switch.
- Condition: This symptom might occur if the controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued.

201809050485

- Symptom: The peer sends IS-IS LSPs with the overload bit set to the switch. When the next hop for reaching the peer changes, the switch calculates a wrong outgoing interface for the traffic to be sent to the peer.
- Condition: This symptom might occur if the peer sends IS-IS LSPs with the overload bit set to the switch and the next hop for reaching the peer changes.

201807160277

- Symptom: When the RPS is installed, the RPS LED is not on, and the display power command does not display the RPS status.
- Condition: This symptom might occur if the RPS is installed.

201810120342

- Symptom: The switch cannot obtain the incoming and outgoing port numbers for traffic on an sFlow-enabled interface.
- Condition: This symptom might occur if sFlow is enabled on an interface.

201810150077

- Symptom: After a two-chassis IRF fabric reboots, MAC authentication users fail authentication on a port of the subordinate member.
- Condition: This symptom might occur if the IRF member devices each have a port that is working in the **userlogin-secure-or-mac** port security mode and MAC authentication users perform authentication on the port on the subordinate member after the IRF fabric reboots.

201809140102

- Symptom: Port security configuration changes after a software upgrade.
- Condition: This symptom might occur if the port security-configured switch is upgraded to R1309P06 or R1309P07.

201812110031

- Symptom: A host is directly connected to the management Ethernet interface of an IRF member device. After an IRF master/subordinate switchover, the host cannot ping the management Ethernet interface.
- Condition: This symptom might occur if the IRF fabric splits and the IRF member device that owns the IRF bridge MAC address fails to re-join the IRF fabric before the IRF bridge MAC persistence timer expires.

Resolved problems in R1309P07

201808290664

- Symptom: In the **display dot1x** command output, the **Offline detect period** field is not aligned with the other fields.
- Condition: This symptom occurs if the **display dot1x** command is executed.

201809050749

- Symptom: Some deleted MAC address entries might remain.
- Condition: This symptom occurs if a large number of MAC address entries are learned and the **undo mac-address** command is used to delete MAC address entries.

201808170356

- Symptom: Mirrored packets are encapsulated with GRE headers when GRE tunnels are not configured.
- Condition: This symptom occurs if flow mirroring is configured.

201808160104

- Symptom: The MIB-Browser fails to read information of the DHCP server MIB nodes.
- Condition: This symptom occurs if the MIB-Browser is used to read information of the DHCP server MIB nodes.

201809050679

- Symptom: The local mirroring configuration does not take effect after the device is rebooted.
- Condition: This symptom occurs if STP is configured globally, local mirroring is configured, and then the device is rebooted.

201808200338

- Symptom: BGP neighbor relationship cannot be established between the specified two link-local addresses.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure link-local addresses for both the local interface and peer interface.
  b. Use the **peer** command to establish BGP neighbor relationship between the two link-local addresses.

201807190555

- Symptom: The NMS memory leaks.
- Condition: This symptom occurs if the **undo snmp-agent trap enable** command is used to disable SNMP notifications and the NMS walks on the SYSLOG-MSG-MIB node information.

201808020501

- Symptom: The device fails to obtain the authorization VLAN name in the \000xxxxx\000 format from the RADIUS server.
- Condition: This symptom might occur if the RADIUS server issues an authorization VLAN name in the \000xxxxx\000 format to an authenticated user.

201807310087

- Symptom: HTTPS redirection fails.
- Condition: This symptom occurs if HTTPS redirection is enabled and a user uses the browser in the MAC OS to access the server.

201806050164

- Symptom: The configuration of a Layer 3 aggregate interface is lost.
- Condition: This symptom occurs if a Layer 3 aggregate interface is configured, the configuration is saved, and the device is rebooted.

201808140119

- Symptom: The ACL function does not take effect.
- Condition: This symptom occurs if 802.1X issues authorization ACLs.

201808070167

- Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. An interface is configured with both MAC authentication and Web authentication.
  b. A user fails to pass MAC authentication.

201808060785

- Symptom: An 802.1X authentication server fails to issue authorization ACLs.
- Condition: This symptom occurs if 802.1X authentication is enabled and the authentication server issues authorization ACLs containing rules related to TCP or UDP services and port numbers to users.

201807210046

- Symptom: After a user logs in to the device by using SSH and then goes offline, remaining information of the user exists on the device.
- Condition: This symptom occurs if the user logs in to the device and then goes offline by using SSH frequently.

201807120164

- Symptom: Some UDP packets with the destination port number 6784 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on an IRF fabric.
  b. The IRF fabric receives UDP packets with the destination port number 6784.

Resolved problems in R1309P06

201804260662

- Symptom: The following problems occur:
  - When a user performs authentication through HWTACACS, the user cannot successfully log in, and no debugging information is printed.
  - When a user performs authentication through RADIUS, the user can successfully log in, but part of the debugging information is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the AAA authentication method as HWTACACS or RADIUS.
  b. A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

201806290399

- Symptom: The value of the snmpEngineboot node is incorrect.
- Condition: This symptom occurs if the whole IRF fabric is rebooted to cause a master/subordinate switchover.

201807160277

- Symptom: The RPS LED is off when the device is connected to an RPS.
- Condition: This symptom occurs when the device is connected to an RPS.

201807040644

- Symptom: PBR does not take effect on ports in a super VLAN.
- Condition: This symptom occurs if PBR is configured on a super VLAN interface.

201712020228

- Symptom: The entPhysicalDescr node value cannot be obtained for the second interface on a 40-G subcard.
- Condition: This symptom occurs if a MIB tool is used to read the value of the entPhysicalDescr node.

201807040637

- Symptom: When the spanning tree protocol is disabled globally, spanning tree protocol packets cannot be flooded.
- Condition: This symptom occurs if the spanning tree protocol is disabled globally.

201807040593

- Symptom: After you modify the login password on the Web interface, you will fail to log in to the device again. In this case, you must set the password again.
- Condition: This symptom occurs if you log in to the device through the Web interface and modify the login password.

201806080831

- Symptom: When a master/subordinate switchover occurs on an IRF fabric, the subordinate member device cannot properly establish the TCP three-way handshake with the peer device. As a result, BGP might flap.
- Condition: This symptom occurs if the IRF fabric has NSR enabled or the subordinate member device is rebooted.

201806080845

- Symptom: In the rd1 table, routes with the same prefix as routes of rd2 are all deleted.
- Condition: This symptom occurs if the following operations are performed:
  a. When VPNv4 routes of rd1 and rd2 are advertised to the peer device, the peer device matches and accepts only VPNv4 routes of rd1.
  b. Withdrawal messages for VPNv4 routes of rd1 and rd2 are advertised to the peer device.
  c. When receiving the withdrawal messages for VPNv4 routes of rd2, the peer device selects VPNv4 routes with the same prefix as VPNv4 routes of rd2 in the rd1 table and deletes these routes.

201806110066

- Symptom: The outgoing interface is incorrectly calculated for an IS-IS route.
- Condition: This symptom occurs if the MAC address of the peer device changes after the peer device establishes the IS-IS neighbor relationship with the local device.

201805250708

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

201804260567

- Symptom: NMS receives traps more than 10 minutes after the device reboots.
- Condition: This symptom occurs if the security model of SNMPv3 is authentication with privacy and the SNMP agent device is rebooted.

201804260682

- Symptom: ISSU upgrade fails.
- Condition: This symptom occurs if ISSU is used to upgrade the software when the **packet-filter** configuration exists.

201806110087

- Symptom: The device might not respond when the **display ike sa** command is executed.
- Condition: This symptom occurs if the device acts as the IKE responder, and IKE SAs are established again after old IKE SAs are aged and deleted.

201806080844

- Symptom: IPsec negotiation fails.
- Condition: This symptom occurs if the VPN instance of the interface bound to an IPsec policy is different from the VPN instance of the IPsec protection process after NAT translation.

201804260604

- Symptom: IPsec tunnels are interrupted irregularly.
- Condition: This symptom occurs if IPsec are configured on two devices and the two devices initiate negotiation packets to each other at the same time.

201711290750

- Symptom: The SNMP function fails.
- Condition: This symptom occurs if the **snmp-agent port** command is used to modify the UDP port for receiving SNMP packets.

201806050863

- Symptom: The command execution result is not displayed.
- Condition: This symptom occurs if you enter the Python shell and execute Comware V7 commands.

201805290211

- Symptom: An access device cannot ping the core device.
- Condition: This symptom occurs if the following operations are performed:
  a. Two devices form an IRF fabric. The IRF fabric is connected to the core device through a multichassis aggregate link.
  b. The access device connects to the IRF fabric through an aggregate interface, and the aggregate interface is assigned to a port isolation group.
  c. Reboot the IRF fabric.

201806140516

- Symptom: ARP replies are dropped.
- Condition: This symptom occurs if a trunk port of the device sends ARP replies shorter than 64 bytes.

201806200110

- Symptom: The system does not automatically modify the QoS priorities for traffic in a voice VLAN.
- Condition: This symptom occurs if an interface has voice VLAN enabled and receives voice traffic.

201805250467

- Symptom: An interface on the device leaves the voice VLAN and cannot join the voice VLAN again.
- Condition: This symptom occurs if the following operations are performed:
  a. In an IRF fabric, an interface on a subordinate member device has LLDP enabled and voice VLAN configured, and is connected to a LLDP/CDP-capable voice device.
  b. Establish or disconnect LLDP neighbor relationship on the subordinate member device.

201805220359

- Symptom: The device continuously sends ARP requests.
- Condition: This symptom occurs if the following operations are performed:
  a. The device is configured with multiport ARP entries.
  b. Outgoing interface consistency check for ARP entries and MAC address entries is enabled.

201805250699

- Symptom: A device port learns the source MAC address in LLDP packets.
- Condition: This symptom occurs if the device port receives LLDP packets.

201806050085

- Symptom: When an LSWM5SP8PM interface card is plugged or unplugged, the interface card name is displayed as LSWM4SP8PM in the device logs.
- Condition: This symptom occurs if an LSWM5SP8PM interface card is plugged or unplugged.

201802010506

- Symptom: An IP address cannot be configured for the device.
- Condition: This symptom occurs if an IRF member device is powered off and rebooted multiple times to perform master/subordinate switchovers.

201804090636

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  a. The network has a large number of short TCP connections.
  b. The device keeps receiving and sending packets.
  c. The device accesses resources that have been released by itself.

201804090093

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  a. A NAT server mapping is configured on an interface. In the mapping, the private IP address of the internal server is the IP address of the interface.
  b. Security control policies are frequently created and deleted when L2TP users access the internal server through the public IP address mapped to the private IP address.

201802010690

- Symptom: The device discards packets with a checksum of 01 00.
- Condition: This symptom might occur if the checksum of incoming packets is 01 00.

201711160780

- Symptom: The energy saving configuration on a combo interface gets lost after the active port of the combo interface changes from the copper port to the fiber port and then back to the copper port.
- Condition: This symptom might occur if the following operations are performed:
  a. When the copper port of the combo interface is active, enable EEE and auto power-down on the combo interface.
  b. Activate the fiber port of the combo interface.
  c. When the fiber port of the combo interface is active, activate the copper port of the combo interface.

201805090571

- Symptom: When dropping unknown multicast data packets is enabled for a VLAN, the device floods multicast packets with TTL 0 in the VLAN.
- Condition: This symptom might occur if dropping unknown multicast data packets is enabled for the VLAN.

201804270451

- Symptom: An interface sends incoming ARP requests back to the source interfaces.
- Condition: This symptom might occur after the following operations are performed:
  a. Configure the interface as an ARP trusted interface by using the arp detection trust command.
  b. Assign the interface to an aggregation group.
  c. Delete the aggregation group or remove the interface from the aggregation group.

201804240510

- Symptom: In an IRF fabric, the displayed MTU value of a Layer 2 aggregate interface on a subordinate device is incorrect.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure the Layer 2 aggregate interface to allow jumbo frames within a specific length to pass through by using the jumboframe enable command.
  b. Save the running configuration and reboot the IRF fabric.

201804180241

- Symptom: The outgoing interface information is inconsistent in the MAC address entry and the ARP entry for the same MAC address.
- Condition: This symptom might occur if the MAC address moves frequently.

201805180576

- Symptom: Symptom: Non-first fragments of an IP packet, which do not contain TCP or UDP port numbers, match an ACL rule specified with TCP or UDP port numbers.
- Condition: This symptom might occur if the ACL rule is specified with TCP or UDP port numbers.

Resolved problems in R1309P03

201801190229

- Symptom: CVE-2017-15896
- Condition: An attacker can exploit this issue to bypass TLS validate and encrypt, send application data to Node.js.

201801190229

- Symptom: CVE-2017-3737
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201801190229

- Symptom: CVE-2017-3738
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201705310258

- Symptom: The device reboots exceptionally at a very low probability.
- Condition: This symptom occurs if the device has been running for a long period of time and invalid memory is accessed when PBR determines whether the next hop is valid through querying the FIB table.

201706300315

- Symptom: When the status of a track entry associated with a static route changes, the static route does not respond to the change, and status of the static route's next hop does not change.
- Condition: This symptom occurs if a static route fails to establish a connection to the track module when the static route is associated with a track entry.

201804090334

- Symptom: It takes 20 seconds to log in to the device through SSH.
- Condition: This symptom occurs if you log in to the device through SSH after the password control feature is enabled.

201705310354

- Symptom: The rawip socket remains, which exhausts the memory and causes the device to reboot.
- Condition: This symptom occurs if you keep performing NQA operation for a period of time.

201802010709

- Symptom: After the **port link-mode route** command is executed on an interface, the command does not take effect.
- Condition: This symptom occurs if the following operations are performed on an IRF fabric:
  a. Disconnect the standby MPU and LPUs of the device in sequence
  b. Restore the connections of the LPUs and standby MPU in sequence.

201706300478

- Symptom: The device cannot send ICMP error packets.
- Condition: This symptom occurs if the following conditions exist:

- The **ip unreachables enable** and **ip ttl-expires enable** commands are configured on the device.
- The device receives ICMP request packets.

201801290865

- Symptom: The prefix obtained from an IPv6 address is still advertised in RA messages.
- Condition: This symptom occurs if an IPv6 address is manually configured and then the **ipv6 nd ra prefix default no-advertise** command is configured to disable the device from advertising the prefix of the IPv6 address.

201802070015

- Symptom: The PoE function of interfaces still supplies power.
- Condition: This symptom occurs if PoE is disabled on all interfaces and then PoE is disabled on the PSE.

201801300024

- Symptom: Some BSR packets are dropped in a VLAN with IGMP snooping enabled.
- Condition: This symptom occurs if IGMP snooping is enabled for a VLAN and BSR packets are received at wire speed in the VLAN.

201803260509

- Symptom: The **bpdu-drop any** command configuration does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  a. On an IRF fabric, configure BFD MAD. Execute the bpdu-drop any command on the IRF physical interfaces.
  b. In system view, execute the undo stp global enable/stp global enable or reboot command. The STP status of interfaces changes.

201803160619

- Symptom: With MAC authentication enabled, the device does not disconnect a user and still displays the user as online when the device does not receive any packets from the user within the offline detection timer but the MAC address entry has not aged out.
- Condition: This symptom occurs if MAC authentication offline detection is enabled and the offline detection timer is different from the MAC address aging timer.

201803200427

- Symptom: Traps are received more than 10 minutes after the device is rebooted.
- Condition: This symptom occurs if the device is rebooted when authentication with privacy is configured for SNMPv3.

201802010956

- Symptom: The connection between an IRF fabric and a controller flaps.
- Condition: This symptom occurs if the following conditions exist:
  - OpenFlow devices form an IRF fabric.
  - A subordinate member device connects to the controller.
  - The subordinate member device receives 150-byte PIM packets at wire speed.

201801300586

- Symptom: An OpenFlow device is disconnected from the controller.
- Condition: This symptom occurs if the controller issues the **openflow shutdown** or **undo openflow shutdown** command twice.

201803230514

- Symptom: After a device configured with port security is rebooted, users fail to come online through MAC authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable port security, and set the port security mode to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt on an interface.
  b. Save the configuration, and delete the .mdb configuration file.
  c. Reboot the device.

201708150559

- Symptom: Dynamic MAC-based VLAN assignment is enabled on an interface, and the PVID of the interface is a secondary VLAN of a primary VLAN. If an incoming frame is tagged with the PVID and fuzzy MAC-to-VLAN entry match succeeds for the frame's source MAC address, the interface cannot forward the frame.
- Condition: This symptom might occur if the interface receives a frame that carries a VLAN ID same as the PVID of the interface, and the PVID is a secondary VLAN of a primary VLAN.

201712220061

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

201712190289

- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

201712190289

- Symptom: CVE-2017-12192
- Condition: Attackers can exploit this issue to cause denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

201712190289

- Symptom: CVE-2017-15274
- Condition: An attacker can exploit this issue to cause a local denial-of-service condition.

201712190289

- Symptom: CVE-2017-15299
- Condition: An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.
-

201801190481

- Symptom: On an OpenFlow-enabled IRF fabric that contains two member switches, the **openflow shutdown** command is executed on an interface of the subordinate switch, and then the interface is brought up from the controller. After a master/subordinate switchover, status of an interface is abnormal on the new master.
- Condition: This symptom might occur if a master/subordinate switchover occurs after an interface that has been shut down by OpenFlow on the subordinate switch is brought up from the controller.

201801190469

- Symptom: On the OpenFlow-enabled switch, execution of the **openflow shutdown** command fails on an aggregate interface.
- Condition: This symptom might occur if the **openflow shutdown** command is executed on an aggregate interface.

201801180979

- Symptom: When receiving PIM bootstrap messages with a length of 1500 bytes, the switch can send only five bootstrap messages per second in a VLAN enabled with IGMP snooping.
- Condition: This symptom might occur if IGMP snooping is enabled for a VLAN.

201712230037

- Symptom: When the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface, the switch forwards the packet by using an incorrect route.
- Condition: This symptom might occur if the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface.

201801040748

- Symptom: ACLs are not completely deleted from the hardware after IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.
- Condition: This symptom might occur if IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.

201801180968

- Symptom: The switch is connected to a VRRP group. After the link between the VRRP master and the switch flaps, the switch has an incorrect ARP entry for the VRRP master.
- Condition: This symptom might occur if the switch is connected to a VRRP group, and the link between the VRRP master and the switch flaps.

201711290635

- Symptom: When a port joins a Layer 2 aggregation group, the allowed jumbo frame length configured on the Layer 2 aggregate interface is not synchronized to that port.
- Condition: This symptom might occur if a port joins a Layer 2 aggregation group that is configured with the allowed jumbo frame length setting.

201712210545

- Symptom: In the output from the **display transceiver diagnosis interface** command, the receive power of transceiver modules is incorrect.
- Condition: This symptom might occur if the **display transceiver diagnosis interface** command is executed.

201711030370

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

201711230489

- Symptom: The device reboots unexpectedly when reading an Entity MIB node.
- Condition: This symptom might occur if the device reads an Entity MIB node.

201711230366

- Symptom: The device reboots unexpectedly after receiving a packet-out message without the output or group action issued by the controller.
- Condition: This symptom might occur if the device receives a packet-out message without the output or group action issued by the controller.

201711230694

- Symptom: The device might fail to delete the configurations of HWTACACS servers when the configurations of HWTACACS servers are frequently deleted. Or, a process exception might occur if the device rolls back the configuration.
- Condition: This symptom might occur if the following conditions exist:
  - The HWTACACS scheme configured on the device contains configurations of multiple HWTACACS authentication, authorization, and accounting servers.
  - The HWTACACS authentication, authorization, or accounting servers have the same VPN instance and IP address settings but different port numbers.

201710100183

- Symptom: When receiving unknown Layer 2 unicast packets of a VLAN, the device floods the packets on all Layer 3 Ethernet subinterfaces and Layer 3 aggregate subinterfaces of which the subinterface number is the same as the VLAN ID.
- Condition: This symptom might occur if Layer 3 Ethernet interfaces or Layer 3 aggregate interfaces have a subinterface of which the subinterface number is the same as the VLAN ID of incoming unknown Layer 2 unicast packets.

201712040081

- Symptom: In an IRF fabric, the console port on the subordinate device hangs and some information of the subordinate device cannot be viewed on the master device.
- Condition: This symptom might occur if the following conditions exist:
  - The IRF fabric is configured with the spanning tree feature.
  - The peer switch is disabled with the spanning tree feature.
  - A loop exists between the IRF fabric and the peer switch.

201711280600

- Symptom: After certain operations are performed, the **display mac-address** command does not display the voice VLAN MAC address entry of an IP phone. When the settings on the interface connected to the IP phone are removed and reconfigured, the IP phone cannot join a voice VLAN.
- Condition: This symptom might occur if the following operations are performed:
  a. Connect an IP phone to an interface.
  b. Configure voice VLAN and port security on the interface.
  c. Remove the settings from the interface and reconfigure them on the interface.

201711280538

- Symptom: MAC address entries of MAC authentication users do not age out after the users go offline.
- Condition: This symptom might occur if the following conditions exist:
  - A Layer 2 switch configured with the spanning tree feature exists between the device and the authentication clients.
  - The device is enabled with MAC authentication.

- The aging timer for dynamic MAC address entries is set to a value greater than 60 seconds by using the **mac-address timer aging** *seconds* command.

201710300395

- Symptom: A remark action conflict is prompted when a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.
- Condition: This symptom might occur if a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.

201711110038

- Symptom: A user fails 802.1X or MAC authentication when the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides
- Condition: This symptom might occur if the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides.

201709250409

- Symptom: The mirroring and STP settings are partially lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Delete some SNMP settings.
  b. Save the configuration by using the save force command and reboot the device.

201708280341

- Symptom: MAC authentication fails after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security, and set the port security mode to userlogin-secure-or-mac on an interface.
  b. Save the configuration and upgrade the software, or reboot the switch and use a .cfg file to restore the configuration.

201708280275

- Symptom: An 802.1X user that passes authentication on an interface is assigned an IP address in the guest VLAN, Auth-Fail VLAN, or critical VLAN instead of an IP address in the authorization VLAN.
- Condition: This symptom might occur if the following conditions exist:
  - Both 802.1X and DHCP are enabled.
  - An 802.1X guest VLAN, Auth-Fail VLAN, or critical VLAN is configured on the interface.
  - The server successfully assigns an authorization VLAN.

201708280259

- Symptom: 802.1X authentication fails on an interface.
- Condition: This symptom might occur if the following operations are performed:
  - Enable 802.1X and specify the port-based access control method on an interface.
  - Set the username request timeout timer by using the **dot1x timer tx-period** *tx-period-value* command.

201708280255

- Symptom: A user logs in to the CLI through a console port. The CLI hangs up after the user executes the **stp edged-port** and **stp loop-protection** commands in interface range view.
- Condition: This symptom might occur if AAA authentication is enabled for CLI login by using the **authentication-mode scheme** command and command accounting is enabled by using the **command accounting** command.

201709250610

- Symptom: In an IRF fabric, the **undo jumbo enable** command configuration loses effect after an ISSU is performed.
- Condition: This symptom occurs after an ISSU is performed.

201710300047

- Symptom: The **snmp-agent target-host trap** command configuration is lost after a master/subordinate switchover is performed in an IRF fabric.
- Condition: This symptom occurs if the *vpn-instance-name* or *security-string* argument in the command contains dots (.).

201708280230

- Symptom: A user passes MAC authentication on an interface with port security configured after failing 802.1X authentication. The user fails MAC authentication after the **shutdown** and **undo shutdown** commands are executed on the interface.
- Condition: This symptom occurs if the port security mode is set to **userlogin-secure-or-mac-ext** on the interface.

201710260388

- Symptom: The device does not support the ACL deployed by the 802.1X authentication server.
- Condition: This symptom occurs when a client performs 802.1X authentication.

201709250739

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

201710200010

- Symptom: Automatic configuration fails because a VLAN interface cannot obtain an IP address.
- Condition: This symptom occurs when the device starts up without a configuration file.

201709220068

- Symptom: The interface view is unavailable on an IRF member device after a master/subordinate switchover.
- Condition: This symptom occurs if new member devices are added during the master/subordinate switchover.

201708310208

- Symptom: Web authentication entries exist, and users of other authentication types fail authentication or fail to get authorized when a large number of users exist.
- Condition: This symptom might occur if the following operations are performed when Web authentication is disabled:
  a. Configure the web-auth free-ip command.
  b. Reboot the device.

201710310028

- Symptom: In an IRF fabric, the RRPP convergence time is 6 to 10 seconds after a master/subordinate switchover is performed upon a master reboot.
- Condition: This symptom occurs if two RRPP domains are configured on the IRF fabric.

201710270144

- Symptom: The device fails to automatically execute the **save force** command.

- Condition: This symptom might occur if the **save force** command is added to the autocfg configuration file.

201704280459

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201704280459

- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

201704270120

- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201705040699

- Symptom: The MAC learning priority settings do not take effect. An interface with low MAC address learning priority can learn the MAC addresses that have been learned by an interface with high MAC address learning priority.
- Condition: This symptom might occur if the source MAC addresses of Layer 2 packets received on the low-priority interface are the same with the high-priority interface.

201707140396

- Symptom: An authenticated user fails MAC authentication when the user attempts to come online again after the switch reboots.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security and set the port security mode of a port to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt.
  b. A user passes MAC authentication on the port.
  c. Save the running configuration to a configuration file, set the configuration file as the next startup configuration file, and delete the .mdb configuration file.
  d. Reboot the switch.

201705120786

- Symptom: When an interface is configured with broadcast, multicast, and unknown unicast storm suppression, the storm suppression thresholds cannot be modified in a specific sequence.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable broadcast, multicast, and unknown unicast storm suppression on an interface and set the storm suppression thresholds in percentage to 0 for the three traffic types.
  b. Change the storm suppression threshold unit for a traffic type from percentage to pps.
  c. Disable unknown unicast storm suppression.

201707260794[FPR-1088]

- Symptom: Traffic forwarding fails because some L3 entries having parity errors cannot berecovered.
- Condition: This symptom might occur if some L3 entries have parity errors.

201708310228

- Symptom: Packet filtering does not work after the switch is rebooted.
- Condition: This symptom might occur if the switch is rebooted after packet filtering is configured.

201710200579

- Symptom: After a Layer 2 extended-link aggregation group is deleted, only one of its former member ports can forward broadcast traffic.
- Condition: This symptom might occur if a Layer 2 extended-link aggregation group is deleted.

201709220068

- Symptom: On an IRF fabric, the view of some interfaces might be unavailable after an IRF master/subordinate switchover.
- Condition: This symptom might occur if an IRF master/subordinate switchover occurs when a new member joins the IRF fabric.

201709040292

- Symptom: With the HWTACACS accounting server being blocked, the switch responds slowly to commands input by a Telnet user.
- Condition: This symptom might occur if HWTACACS authentication is enabled for login.

201710270540

- Symptom: Certain QoS policies cannot be applied.
- Condition: This symptom might occur if one of the following operations are performed.
  - Apply a QoS policy that matches the outer VLAN IDs or inner VLAN IDs to the inbound direction of an interface for outer VLAN ID remarking.
  - Apply a QoS policy that matches the inner VLAN IDs to the inbound direction of an interface for inner VLAN ID remarking.
  - Apply a QoS policy that matches the outer VLAN IDs to the outbound direction of an interface for inner VLAN ID remarking.

201710200099

- Symptom: sFlow cannot collect outgoing traffic statistics on an interface.
- Condition: This symptom might occur if sFlow is configured on an interface.

201709250190

- Symptom: In a Layer 2 extended-link aggregation group, broadcast traffic received by a member port is forwarded out of the other member ports.
- Condition: This symptom might occur if a member port of a Layer 2 extended-link aggregation group receives broadcast traffic.

201709010571

- Symptom: LLDP is enabled globally and on an interface. The LLDPDUs sent by the interface show that autonegotiation is supported and enabled, but the PMD parameter Auto-negotiated Advertised Capability field is all zeros.
- Condition: This symptom might occur if LLDP is enabled globally and on an interface.

Resolved problems in R1309

201704280459

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201704280459

- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

201704270120

- Symptom: CVE-2014-9297
- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201707260794

- Symptom: Forwarding errors or traffic interruptions might occur on the switch.
- Condition: This symptom occurs with a low probability if the switch runs for a long time.

201707200766

- Symptom: During automatic ADCampus deployment, the switch does not replace the configuration on a downlink interface with the trunk port configuration when an AP accesses the switch through the downlink interface.
- Condition: This symptom might occur if the switch acts as an access node on the ADCampus network.

201707170566

- Symptom: The value of the **MaxPower** field is incorrect in the output from the **display poe device** command.
- Condition: This symptom might occur if the switch is enabled with PoE.

201707170562

- Symptom: In an IRF fabric, IRF physical interfaces keep receiving packets with a CRC error.
- Condition: This symptom might occur if fixed 40-GE ports on the switch panel are used as the IRF physical interfaces.

201707150289

- Symptom: When uRPF is globally enabled, the switch does not forward packets of which the source IP addresses match the destination addresses of non-direct routing entries.
- Condition: This symptom might occur if the switch is globally enabled with uRPF.

201703090716

- Symptom: The DHCP snooping trusted port configuration does not take effect on an aggregate interface on a multi-chassis IRF fabric.

- Condition: This symptom might occur if the following operations are performed on the IRF fabric:
  a. Configure an aggregate interface as a DHCP snooping trusted port.
  b. Initiate an IRF master/subordinate switchover. Or, save the running configuration and reboot the IRF fabric.

Resolved problems in R1308

None

Resolved problems in R1121P05

201612270435

- Symptom: Memory leaks occur.
- Condition: This symptom occurs if you shut down and bring up an interface frequently or the interface receives a large number of TCN BPDUs.

Resolved problems in R1121P03

201610140261

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

201610140261

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

Resolved problems in R1121P02

201610260405

- Symptom: A user fails to log in to the switch in SSH or Telnet method.
- Condition: This symptom occurs if the following conditions exist:
  - The switch is configured with the tcp syn-cookie enable command.
  - The SSH/Telnet client is not directly connected to the switch.
  - A user remotely logs in to the switch by using the IPv6 address of the switch in SSH or Telnet method.

201607180428

- Symptom: IS-IS neighbor relationship can be established between a switch and a Cisco NX9000 device. However, the switch cannot get routing information.
- Condition: This symptom occurs if the following conditions exist:
  - The switch and the Cisco NX9000 device are connected by using IS-IS.
  - The length of the MT IS TLV in protocol packets sent by the Cisco NX9000 device is 2 bytes. The switch considers the LSPs as invalid and drops them.

201603280338

- Symptom: The switch and the firewall module installed in the switch might fail to ping each other.
- Condition: This symptom occurs if the firewall module LSPM6FWD is repeatedly rebooted.

201607080484

- Symptom: The enhanced CDP feature deletes unauthenticated voice users.
- Condition: This symptom occurs if the MAC authentication delay feature is enabled.

201606210088

- Symptom: A voice VLAN user cannot join the critical voice VLAN.
- Condition: This symptom occurs if the switch receives CDP packets from some IP phones.

201611210490

- Symptom: An interface on an LSWM2SP2PM interface card cannot come up.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has an LSWM2SP2PM interface card installed.
  - MACsec is configured on an interface of the interface card.
  - The switch is rebooted.

201610240043

- Symptom: The configuration fails to be saved.
- Condition: This symptom occurs if the **storm-constrain** command configuration flag bit in the memory is modified.

201610150088

- Symptom: A user cannot access the network after passing MAC authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable MAC authentication for access users.
  b. Enable MAC move.
  c. Configure an IRF fabric and then forward traffic on only one IRF member device.

201610100067

- Symptom: A TFTP operation failure log is displayed even if the TFTP operation succeeds.
- Condition: This symptom occurs if a TFTP operation is performed.

201610310115

- Symptom: The speed of a 1000-Mbps port is negotiated as 100 Mbps when it is connected to a 1000-Mbps NIC.
- Condition: This symptom occurs if a 1000-Mbps copper port is connected to a 1000-Mbps NIC of a server.

Resolved problems in R1121P01

201607280524

- Symptom: CVE-2016-2177
- Condition: Fixed vulnerability in s3_srvr.c, ssl_sess.c, and t1_lib.c functions in OpenSSL through 1.0.2h that allows remote attackers to cause a denial of service (integer overflow and

application crash), or possibly have an unspecified other impact by leveraging unexpected malloc behavior.

201608290241

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

201609060439

- Symptom: BFD MAD is in faulty state on an IRF fabric when certain conditions exist.
- Condition: This symptom might occur if BFD MAD is configured on an IRF fabric and its peer, and the IRF fabric can receive BFD packets from the peer.

201609230495

- Symptom: After frequent Telnet or SSH logins and logouts, the following symptoms might occur when the patch for the comsh process is installed:
  - In standalone mode, patch installation takes a long period of time.
  - In IRF mode, if the patch is first installed on the master, patch installation takes a long period of time; if the patch is first installed on subordinates, patch installation fails on the master.
- Condition: This symptom might occur if frequent Telnet or SSH logins and logouts are performed.

201608110180

- Symptom: On an IRF fabric, when the memory usage of the master exceeds the upper limit, BGP NSR might have unrecoverable errors.
- Condition: This symptom might occur if BGP is configured on an IRF fabric, and the memory usage of the master exceeds the upper limit.

201606270545

- Symptom: When multiple MD5 authentication modes are configured for an OSPF area, the switch has PW errors and fails to establish neighbor relationships after a reboot.
- Condition: This symptom might occur if multiple MD5 authentication modes are configured for an OSPF area.

201607180448

- Symptom: When a traceroute operation is performed on a remote device, and the switch is on the path to the destination, the remote device cannot detect the switch, and the switch displays the "ICMP Discard: ICMP reached rate limit." message.
- Condition: This symptom might occur if a traceroute operation is performed on a remote device, and the switch is on the path to the destination.

201610130001

- Symptom: In the help information of the **mtu** command, the MTU value range is incorrect.
- Condition: This symptom might occur if the help information is displayed for the **mtu** command.

201609210504

- Symptom: In the help information of the **jumboframe enable** command, the maximum frame length is not 12000.
- Condition: This symptom might occur if the help information is displayed for the **jumboframe enable** command.

201607220132

- Symptom: After the switch is powered off and rebooted, information is modified for some transceiver modules that are not write-protected, and the transceiver modules become unavailable because of damage.
- Condition: This symptom might occur if the switch is powered off and rebooted.

201606270084

- Symptom: The switch does not process EAPOL v3 packets of 802.1X authentication and displays the "Invalid protocol version ID" message.
- Condition: This symptom might occur if the switch receives EAPOL v3 packets of 802.1X authentication.

201609280505

- Symptom: The settings of a RADIUS scheme are saved twice on an IRF fabric. After a master/subordinate switchover, the RADIUS scheme settings are lost.
- Condition: This symptom might occur if the settings of a RADIUS scheme are saved twice on an IRF fabric, and a master/subordinate switchover occurs.

201608110180

- Symptom: The status of BGP NSR is not correct and cannot recover.
- Condition: This symptom occurs if BGP NSR is configured for an IRF fabric and the memory threshold is reached.

201607180405

- Symptom: The CLI hangs.
- Condition: This symptom occurs if the following conditions exists:
  - CDP compatibility for LLDP is enabled on the device.
  - A port is configured to be shut down upon receiving an illegal frame.
  - The port is connected to a Cisco telephone, and the telephone fails authentication.

201609010307

- Symptom: No authentication page is pushed when a user performs portal authentication.
- Condition: This symptom occurs if the following conditions exist:
  - Portal authentication is configured on the device.
  - The user tries to access the external network through a Web browser on the PC connected to the device.

201609030158

- Symptom: The device does not receive any OpenFlow entries from the OpenFlow controller.
- Condition: This symptom occurs if the OpenFlow controller is an open-source SDN controller.

201607270178

- Symptom: 802.1X or MAC authentication users on an IRF fabric cannot come online.
- Condition: This symptom occurs if the following conditions exist:
  - The maximum number of 802.1X or MAC authentication users on the IRF fabric is reached.
  - The users that pass 802.1X or MAC authentication but do not obtain authorized rights go offline, because an IRF master/subordinate switchover occurs or interfaces go down.

201609130493

- Symptom: An error message does not end with a new line character.

- Condition: This symptom occurs when you associate an interface that does not support VPN with a VPN instance.

Resolved problems in R1121

201605040255

- Symptom: CVE-2015-8138
- Condition: Fixed vulnerability in ntpd which attackers may be able to disable time synchronization by sending a crafted NTP packet to the NTP client.

201605040255

- Symptom: CVE-2015-7979
- Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.

201605040255

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201605040255

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201607280521

- Symptom: CVE-2012-0036
- Condition: Fixed vulnerability in curl and libcurl 7.2x before 7.24.0 that allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.

201606280241

- Symptom: CVE-2016-4953
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.

201606280241

- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.

201606280241

- Symptom: CVE-2016-4956
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

01608260185

- Symptom: The new master device in an IRF fabric hangs after a master/subordinate switchover.
- Condition: This symptom occurs if the following tasks are performed:
  a. Reboot the master device in the IRF fabric. A master/subordinate switchover occurs.
  b. Wait for IRF physical interfaces on the previous master device to come up.
  c. Walk MIB node hh3cStackPortStatus.

201609070244

- Symptom: PD detection and classification on a port are affected after PoE performs power negotiation on the port.
- Condition: None.

201606270528

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if a user with an ultra-long username Telnets to the device.

201606270484

- Symptom: The description configuration for an interface fails, but no error message is displayed.
- Condition: This symptom occurs if the description contains Chinese characters.

201606070262

- Symptom: The device configured with OpenFlow inband management VLANs cannot establish OSPF or OSPFv3 neighbor relationships with other devices.
- Condition: This symptom occurs if the device is configured with OpenFlow inband management VLANs.

201608170255

- Symptom: Packet statistics for a management Ethernet interface are incorrect.
- Condition: This symptom occurs if the statistics are obtained through MIB.

201607190428

- Symptom: The speed autonegotiation configuration is lost.
- Condition: This symptom occurs if the .mdb next-startup configuration file is deleted and the device starts up with a .cfg next-startup configuration file.

201607110099

- Symptom: Maximum PI power negotiation fails on an interface configured with PoE.
- Condition: This symptom occurs if the maximum PI power is automatically deployed on the interface and the device is rebooted after the configuration is saved.

201607040331

- Symptom: A user that fails MAC authentication cannot be assigned to the MAC authentication critical VLAN on the access port of the user.
- Condition: This symptom occurs if the following conditions exists:
  - The user fails MAC authentication and is assigned to the MAC authentication guest VLAN on the port.
  - The authentication server becomes unreachable.
  - Users are removed from the MAC authentication guest VLAN on the port by using the reset mac-authentication guest-vlan command.

Resolved problems in R1120P10

201606150036

- Symptom: After the switch is powered off and then rebooted, some transceiver modules without write protection are damaged.
- Condition: This symptom might occur if the switch is powered off and then rebooted.

201605120341

- Symptom: Traffic forwarding fails because some L3 entries having parity errors cannot be recovered.
- Condition: This symptom might occur if some L3 entries have parity errors.

201604180493

- Symptom: ACLs that use a rule containing the **established** parameter do not take effect when they are used with 802.1X authentication or MAC authentication.
- Condition: This symptom might occur if 802.1X authentication or MAC authentication is enabled.

201604120327

- Symptom: The switch does not generate the MAC_TABLE_FULL_PORT log message when the MAC learning limit is reached on an interface enabled with voice VLAN.
- Condition: This symptom might occur if the **mac-address max-mac-count** command is configured on an interface enabled with voice VLAN.

201606210245

- Symptom: In the output from the **display ip routing-table** command, OSPF internal routes and external routes are not differentiated.
- Condition: This symptom might occur if the **display ip routing-table** command is executed.

201606060110

- Symptom: A ping operation through a management Ethernet interface fails when ICMP echo requests are longer than 1472 bytes.
- Condition: This symptom might occur if a ping operation is performed through a management Ethernet interface and ICMP echo requests are longer than 1472 bytes.

201604180513

- Symptom: When inactivity aging of port security is enabled on an interface, a sticky MAC address ages out before the secure MAC aging timer expires.
- Condition: This symptom might occur if the following conditions exist on an interface:
  - Port security and inactivity aging are enabled.
  - The port-security timer autolearn aging command is used to set the secure MAC aging timer.

201603190339

- Symptom: When RADIUS server load sharing is enabled, multiple RADIUS packets for one 802.1X EAP authentication process are sent to different RADIUS servers.
- Condition: This symptom might occur if RADIUS server load sharing is enabled.

201604180531

- Symptom: A PC cannot join the 802.1X guest VLAN.
- Condition: This symptom occurs if the following conditions exist:

- Both 802.1X authentication and MAC authentication are enabled on the device.
- The device connects to multiple PCs through a hub.
- The PC fails MAC authentication.

201607020041

- Symptom: The entPhysicalModelName node displays the information for the subslot instead of the information for CPU 0 in slot 1 during a MIB walk.
- Condition: This symptom occurs if a MIB walk is performed on the entPhysicalModelName node.

201606230218

- Symptom: Dynamically learned secure MAC addresses of a port cannot be deleted after the port goes down.
- Condition: This symptom occurs if the port is enabled with the dynamic secure MAC feature.

201606220123

- Symptom: A user that fails 802.1X authentication for the first time fails subsequent 802.1X authentication.
- Condition: This symptom occurs if the user comes online after passing MAC authentication and then performs 802.1X authentication.

201604260373

- Symptom: The actual period of traffic interruption is three seconds rather than six seconds after a port is disconnected and then reconnected.
- Condition: This symptom occurs if the LACP short timeout interval is set for the port.

201605090524

- Symptom: CVE-2015-7979
- Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.

201605090524

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201605090524

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201606070567

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070567

- Symptom: CVE-2016-2106

- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070567

- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.02h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.

201606070567

- Symptom: CVE-2016-2108
- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).

201606070567

- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

201606070567

- Symptom: CVE-2016-2176
- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service

201605170546

- Symptom: CVE-2016-1547
- Condition: Fixed vulnerability where an off-path attacker can deny service to ntpd clients by demobilizing preemptable associations using spoofed crypto-NAK packets.

201605170546

- Symptom: CVE-2016-1548
- Condition: Fixed vulnerability where an attacker can change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode.

201605170546

- Symptom: CVE-2016-1550
- Condition: Fixed vulnerability in ntpd function allow an attacker to conduct a timing attack to compute the value of the valid authentication digest causing forged packets to be accepted by ntpd.

201605170546

- Symptom: CVE-2016-1551
- Condition: Fixed vulnerability in ntpd allows unauthenticated network attackers to spoof refclock packets to ntpd processes on systems that do not implement bogon filtering.

201605170546

- Symptom: CVE-2016-2519
- Condition: Fixed vulnerability in ntpd will abort if an attempt is made to read an oversized value.

201605170546

- Symptom: CVE-2015-7704
- Condition: Fixed vulnerability in ntpd that a remote attacker could use, to send a packet to an ntpd client that would increase the client's polling interval value, and effectively disable synchronization with the server.

Resolved problems in R1120P07

201601140410

- Symptom: When TCP port X is enabled, TCP port X + 2048*N is also enabled (N is an arbitrary integer).
- Condition: This symptom occurs if TCP port X is enabled, for example, TCP port 23 is enabled by using the **telnet server enable** command.

201602150295

- Symptom: After the switch is rebooted, the configuration for queue **a** in a custom queue scheduling profile is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use the qos qmprofile command to create a custom queue scheduling profile.
  b. Configure queue a to use SP queuing.
  c. Modify the queuing configuration to WRR or WFQ for queue a.
  d. Save the configuration and reboot the switch.

201603190098

- Symptom: If you assign a Layer 2 Ethernet interface to Layer 2 aggregation group 2 after assigning it to Layer 2 aggregation group 1, the configuration fails, and all link aggregation group configuration on the interface is deleted.
- Condition: This symptom occurs if the following operations are performed:
  a. Assign a Layer 2 Ethernet interface to Layer 2 aggregation group 1.
  b. Assign the interface to Layer 2 aggregation group 2.

201603110390

- Symptom: The message "The operation completed unsuccessfully." appears when the **undo port auto-power-down** command is executed on an interface.
- Condition: This symptom occurs if the **undo port auto-power-down** command is executed on an interface.

201603160134

- Symptom: A DHCP client cannot obtain an IP address.
- Condition: This symptom occurs if the following conditions exist:
  - DHCP snooping is enabled on a switch.
  - DHCP request messages are forwarded across VLANs on the DHCP snooping-enabled switch.

201603180570

- Symptom: After a PC joins the critical VLAN, the PC is reauthenticated about every 20 seconds.
- Condition: This symptom occurs if the 802.1X server is unreachable when the PC performs 802.1X authentication.

201604210202

- Symptom: A PC is logged out immediately after the PC successfully comes online through 802.1X authentication.
- Condition: This symptom occurs if the following conditions exist:
  - An IP phone comes online through MAC authentication.
  - The PC is connected to the switch through the IP phone.
  - The PC performs 802.1X authentication, and no authorization VLAN is assigned to the PC.

201604180493

- Symptom: When an ACL of the established type is issued, the system prompts that the ACL is not supported.
- Condition: This symptom occurs if 802.1X or MAC authentication is enabled and the switch issues an ACL of the established type.

201603190309

- Symptom: The **dot1x re-authenticate server-unreachable keep-online** command configuration does not take effect. When the server is unreachable, the user is reauthenticated and then logged out.
- Condition: This symptom occurs if the **dot1x re-authenticate server-unreachable keep-online** command is configured and the session timeout timer is triggered after the user comes online.

201603180515

- Symptom: CVE-2016-0701
- Condition: Fixed vulnerability in the DH_check_pub_key function which makes it easier for remote attackers to discover a private DH (Diffie-Hellman) exponent by making multiple handshakes with a peer that chose an inappropriate number. This issue affects OpenSSL version 1.0.2. and addressed in 1.0.2f. OpenSSL 1.0.1 is not affected by this CVE.

201603180515

- Symptom: CVE-2015-3197
- Condition: Fixed vulnerability when using SSLv2 which can be exploited in a man-in-the-middle attack, if device has disabled ciphers.

201603230415

- Symptom: CVE-2016-0705
- Condition: Fixed vulnerability when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources.

201603230415

- Symptom: CVE-2016-0798
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt.

201603230415

- Symptom: CVE-2016-0797
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference).

201603230415

- Symptom: CVE-2016-0799
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service which could lead to memory allocation failure or memory leaks.

201603230415

- Symptom: CVE-2016-0702
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g which makes it easier for local users to discover RSA keys leveraging cache-bank conflicts, aka a "CacheBleed" attack.

201604110488

- Symptom: CVE-2016-2842
- Condition: Fixed vulnerability in the doapr_outch function in crypto/bio/b_print.c, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string.

201604060219

- Symptom: When DHCP server and DHCP snooping settings are configured on the switch, DHCP clients can obtain IP addresses, but the switch cannot generate DHCP snooping entries.
- Condition: This symptom might occur if DHCP server and DHCP snooping settings are configured on the switch.

201603090119

- Symptom: An ACL rule takes effect 25 seconds later than the start time of the time range specified for the rule.
- Condition: None.

201512110325

- Symptom: The listening TCP port configuration on a local portal Web server changes to the default setting after the local portal Web server view is re-entered.
- Condition: This symptom occurs if the local portal Web server uses HTTPS to exchange authentication information with clients.

201601260436

- Symptom: A dynamic aggregate interface goes down and then comes up after the receiver or transmitter of the transceiver module on one of its member port is removed.
- Condition: This symptom occurs if BFD is configured on the aggregate interface.

201601050377

- Symptom: The **switch-mode** command configuration for ARP tables does not take effect on VLAN interfaces configured as customer-side ports by using the **arp mode uni** command.
- Condition: None.

201603010069

- Symptom: The **Session timeout period** field in the **display mac-authentication connection** command output displays **N/A**.
- Condition: This symptom might occur if the authentication server assigns the Session-Timeout attribute.

201603160269

- Symptom: The switch fails to establish an LDP LSP with the peer device after LDP is disabled and then enabled on the peer port.
- Condition: This symptom occurs if the peer port is configured with a secondary IP address.

Resolved problems in R1120

201512290191

- Symptom: CVE-2015-3194
- Condition: The signature verification routines will crash with a NULL pointer dereference, if presented with an ASN.1 signature using the RSA PSS algorithm and absent mask generation function parameter. This can be used to crash any certificate verification operation and exploited in a DoS attack.

201512290191

- Symptom: CVE-2015-3195
- Condition: When presented with a malformed X509_ATTRIBUTE structure OpenSSL will leak memory. This structure is used by the PKCS#7 and CMS routines so any application which reads PKCS#7 or CMS data from untrusted sources is affected.

201512290191

- Symptom: CVE-2015-3196
- Condition: If PSK identity hints are received by a multi-threaded client then the values are wrongly updated in the parent SSL_CTX structure. This can result in a race condition potentially leading to a double free of the identify hint data.

201512290191

- Symptom: CVE-2015-1794
- Condition: If a client receives a ServerKeyExchange for an anonymous DH ciphersuite with the value of p set to 0 then a seg fault can occur leading to a possible denial of service attack.

201512150528

- Symptom: NTP clock synchronization fails.
- Condition: This symptom occurs if the switch is connected to an NTP-enabled Cisco device.

201603010337

- Symptom: After a static default route is configured, packets destined for invalid class-E IP addresses are forwarded rather than dropped.
- Condition: This symptom occurs if a static default route is configured and the switch receives packets destined for invalid class-E IP addresses.

201602150295

- Symptom: After the switch is rebooted, the configuration for a queue in a user-defined queue scheduling profile is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use the qos qmprofile command to create a user-defined queue scheduling profile.
  b. Configure the queuing method as SP for the queue in the queue scheduling profile.
  c. Modify the queuing method to WRR or WFQ for the queue in the queue scheduling profile.
  d. Save the configuration and reboot the switch.

201510300359

- Symptom: When an MAC authentication user is online, an 802.1X user goes offline immediately after the user passes 802.1X authentication and comes online.
- Condition: This symptom occurs if MAC authentication and 802.1X authentication assign the same VLAN to users.

201509220038

- Symptom: User authentication fails.
- Condition: This symptom occurs if the switch uses an ACS 5.6 server to perform AAA authentication.

Resolved problems in R1118P02

201511200517

- Symptom: CVE-2015-7871
- Condition: Cause NTPD to accept time from unauthenticated peers.

201511200517

- Symptom: CVE-2015-7704
- Condition: An NTPD client forged by a DDoS attacker located anywhere on the Internet, which can exploit NTP's to disable NTP at a victim client or it may also trigger a firewall block for packets from the target machine.

201511200517

- Symptom: CVE-2015-7705
- Condition: The DDoS attacker can send a device a high volume of NTPD queries that are spoofed to look like they come from the client. The servers then start rate-limiting the client.

201511200517

- Symptom: CVE-2015-7855
- Condition: NTPD mode 6 or mode 7 packets containing an unusually long data value could possibly use cause NTP to crash, resulting in a denial of service.

201512290083

- Symptom: The **dot1x after-mac-auth max-attempt** command configuration is incorrectly displayed.
- Condition: This symptom might occur if the **dot1x after-mac-auth max-attempt** command is executed.

201512170304

- Symptom: The **boot-loader file** command fails to upgrade the software for all member switches of an IRF fabric at the same time.
- Condition: This symptom might occur if the **boot-loader file** command is used to upgrade the software for all member switches of an IRF fabric at the same time.

201510260061

- Symptom: Users fail 802.1X authentication if the PEAP method is used.
- Condition: This symptom might occur if the PEAP method is used.

Resolved problems in R1118

201511090144

- Symptom: A Cisco IP phone leaves the voice VLAN after LLDP neighbor ages out and the voice VLAN aging timer expires.
- Condition: This symptom occurs if the switch advertises voice VLAN information to the IP phone.

Resolved problems in R1111P01

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 5130 HI Switch Series Installation Guide

- HPE PSR720-56A Power Supply User Guide
- HPE PSR1110-56A Power Supply User Guide
- HPE PSR150-A & PSR150-D Power Supplies User Guide
- HPE LSWM2SP2PM Interface Card (JH157A) User Guide
- HPE LSWM2XGT2PM Interface Card (JH156A) User Guide
- HPE 5130 HI Switch Series Configuration Guides-Release 1121
- HPE 5130 HI Switch Series Command References-Release 1121

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

Please refer to:

- HPE FlexNetwork 5130 HI Switch Series Installation Guide

Software features

Table 5 Software features of the 5130HI series

Feature	HPE 5130 24G 4SFP+ 1-slot HI Switch JH323A HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A	HPE 5130 48G 4SFP+ 1-slot HI Switch JH324A HPE 5130 48G PoE+ 4SFP+ 1-slot HI Switch JH326A
Full duplex Wire speed L2 switching capacity	168Gbps	216Gbps
Whole system Wire speed L2 switching Packet forwarding rate	125Mpps	160.71Mpps
IRF	• Ring topology • Daisy chain topology • LACP MAD • ARP MAD • ND MAD • BFD MAD	
Link aggregation	• Aggregation of GE ports • Aggregation of 10-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 • Back pressure	
Jumbo Frame	• Supports maximum frame size of 10000	
MAC address table	• 32K MAC addresses • 1K static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port	

Feature	HPE 5130 24G 4SFP+ 1-slot HI Switch JH323A HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A	HPE 5130 48G 4SFP+ 1-slot HI Switch JH324A HPE 5130 48G PoE+ 4SFP+ 1-slot HI Switch JH326A
VLAN	• Port-based VLANs (4094 VLANs) • QinQ and selective QinQ • Voice VLAN • protocol-vlan • MAC vlan	
VLAN mapping	• One-to-one VLAN mapping • Many-to-one VLAN mapping • Two-to-two VLAN mapping	
ARP	• 8K entries • 2K static entries • Gratuitous ARP • Common proxy ARP and local proxy ARP • ARP source suppression • ARP black hole • ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings) • Multiport ARP	
ND	• 4K entries • 2K static entries • ND Snooping	
VLAN virtual interface	1K	
DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server • DHCP Option82 • DHCPv6 server • DHCPv6 relay agent • DHCPv6 snooping	
UDP helper	• UDP helper	
DNS	• Static DNS • Dynamic DNS • IPv4 and IPv6 DNS	
unicast route	• IPv4/IPv6 static routes • RIP/RIPng • Routing policies	
BFD	• Static route • MAD	
Multicast	• IGMP snooping • MLD snooping • IPv4 and IPv6 multicast VLAN • IPv4 and IPv6 PIM snooping	

Feature	HPE 5130 24G 4SFP+ 1-slot HI Switch JH323A HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A	HPE 5130 48G 4SFP+ 1-slot HI Switch JH324A HPE 5130 48G PoE+ 4SFP+ 1-slot HI Switch JH326A
Broadcast/multicast /unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Bps-based storm control	
MSTP	• STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard	
SmartLink	• 32	
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/WDRR/WFQ queue scheduling algorithms • Port-based rate limiting • Flow-based redirection • Time range	
Mirroring	• Stream mirroring • Port mirroring • Multiple mirror observing port • Port remote mirroring (RSPAN)	
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 2,048 users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • Dynamic 802.1X-based QoS/ACL/VLAN assignment	
Open Flow	• 16 Instance • MAC-IP	
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)	

Feature	HPE 5130 24G 4SFP+ 1-slot HI Switch JH323A HPE 5130 24G PoE+ 4SFP+ 1-slot HI Switch JH325A	HPE 5130 48G 4SFP+ 1-slot HI Switch JH324A HPE 5130 48G PoE+ 4SFP+ 1-slot HI Switch JH326A
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • IMC NMS • System log • Hierarchical alarms • NTP • Power supply alarm function • Fan and temperature alarms	
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track • Remote maintenance through Telnet • 802.1ag • 802.3ah • DLDP • Virtual Cable Test	

Appendix B Fixed security vulnerabilities

Fixed security vulnerabilities in R3507P09

CVE-2015-2808

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah"

Fixed security vulnerabilities in R3507P06

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-2021-4160

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).

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.

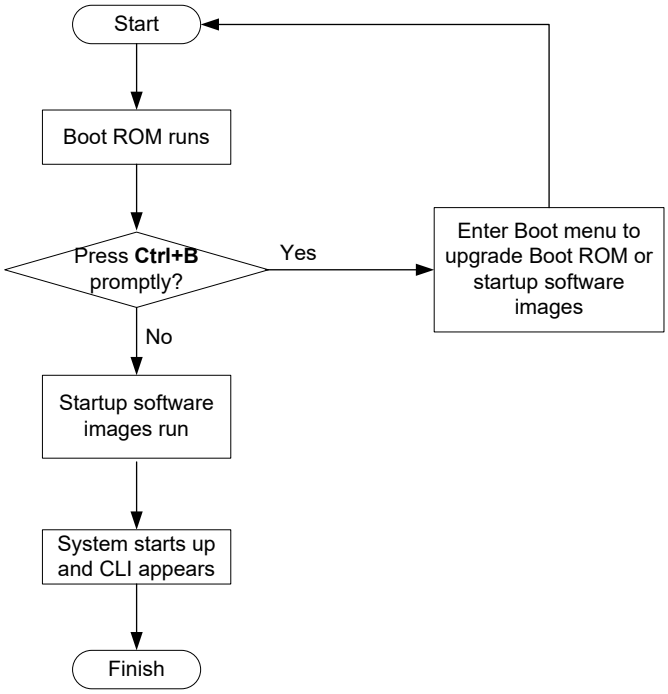
  The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

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, *5130HI-CMW710-BOOT-Rxxxx.bin* and *5130HI-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 5130HI 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 10.10.110.1
Connected to 10.10.110.1.
220 FTP service ready.
User(10.10.110.1:(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 so
ftware 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 so
ftware 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 6.

Table 6 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 5130 24G PoE+ 4SFP+ 1-slot HI BOOTROM, Version 111        *
*                                                                              *
********************************************************************************
Copyright (c) 2010-2015 Hewlett-Packard Development Company, L.P.

Creation Date       : Feb  3 2015, 19:43:00
CPU Clock Speed     : 1000MHz
Memory Size         : 2048MB
Flash Size          : 512MB
CPLD Version        : 001
PCB Version         : Ver.A
Mac Address         : 70f96dfacbda


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

Press one of the shortcut key combinations at prompt.

Table 7 Shortcut keys

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

Shortcut keys	Prompt message	Function	Remarks
Ctrl+D	Press Ctrl+D to access BASIC BOOT MENU	Accesses the basic Boot menu.	Press the keys within 1 seconds after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.

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 111                          *
*                                                                              *
********************************************************************************

   BASIC BOOT MENU

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

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

Table 8 Basic Boot ROM menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see 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.

Option	Task
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 9).

Table 9 BASIC ASSISTANT menu options

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

Accessing the extended Boot menu

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

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

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 10). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 5130HI 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

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

Table 10 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	• Specify the main and backup software image file for the next startup. • Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+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 11.

Table 11 EXTENDED ASSISTANT menu options

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

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 12 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

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 13 FTP parameter description

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

NOTE:

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

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

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

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

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 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.

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
```

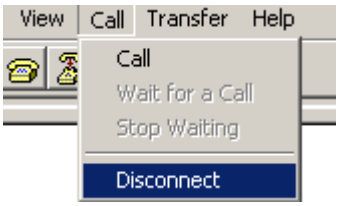
3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

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

```
Press enter key when ready
```

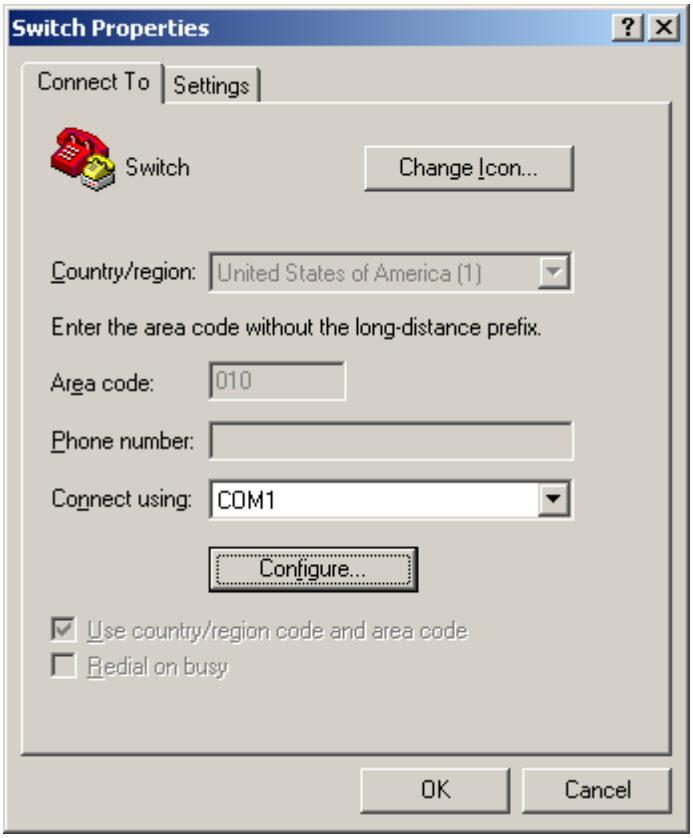
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



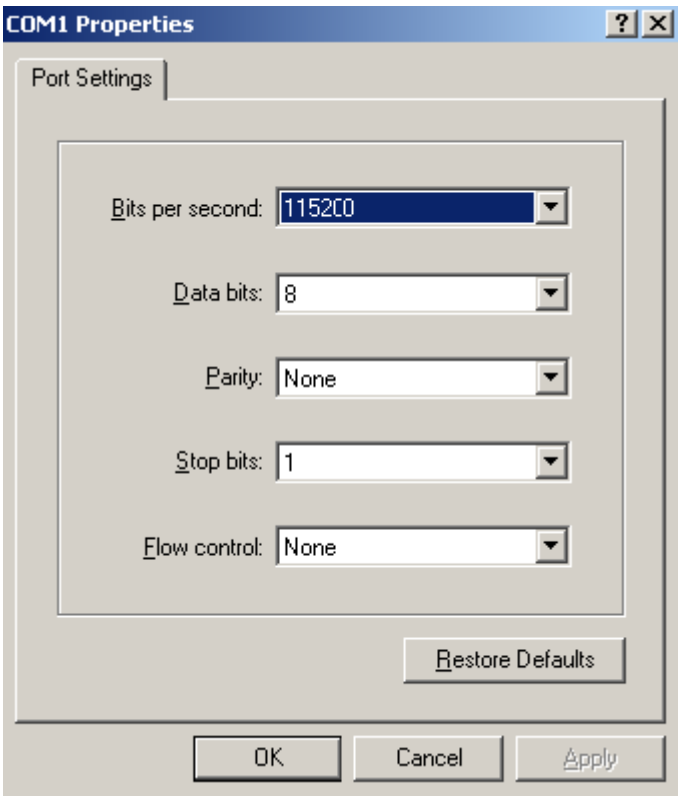
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



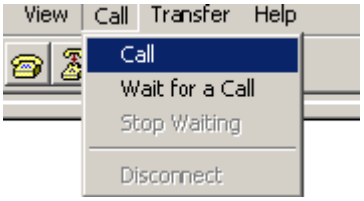
   c. Select 115200 from the Bits per second list and click OK.

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:

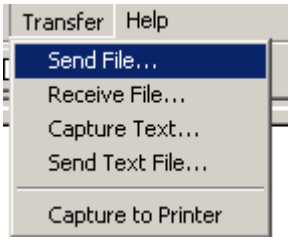
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

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 ...CCCCCCCCCCCCCCCCCCCCCCCCC
```

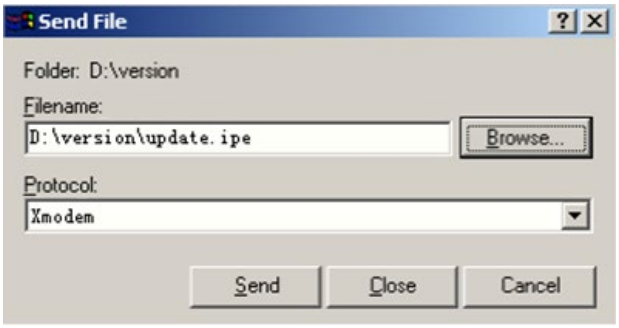
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 6 Transfer menu



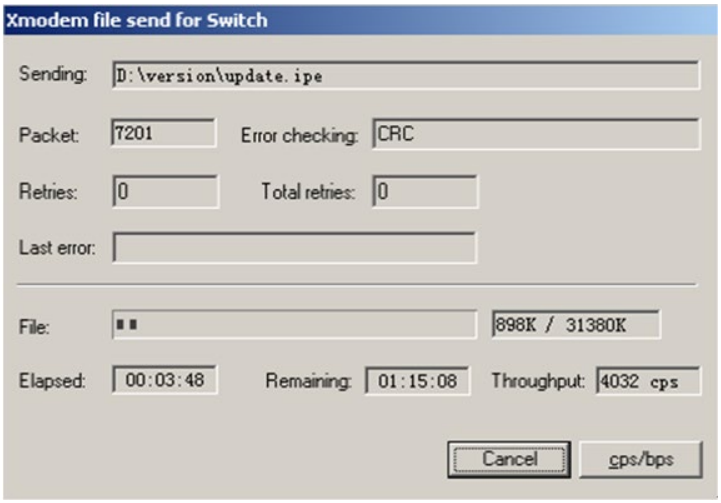
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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

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 14 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 15 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.

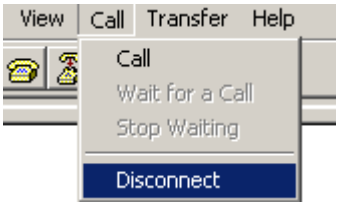
```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

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
```

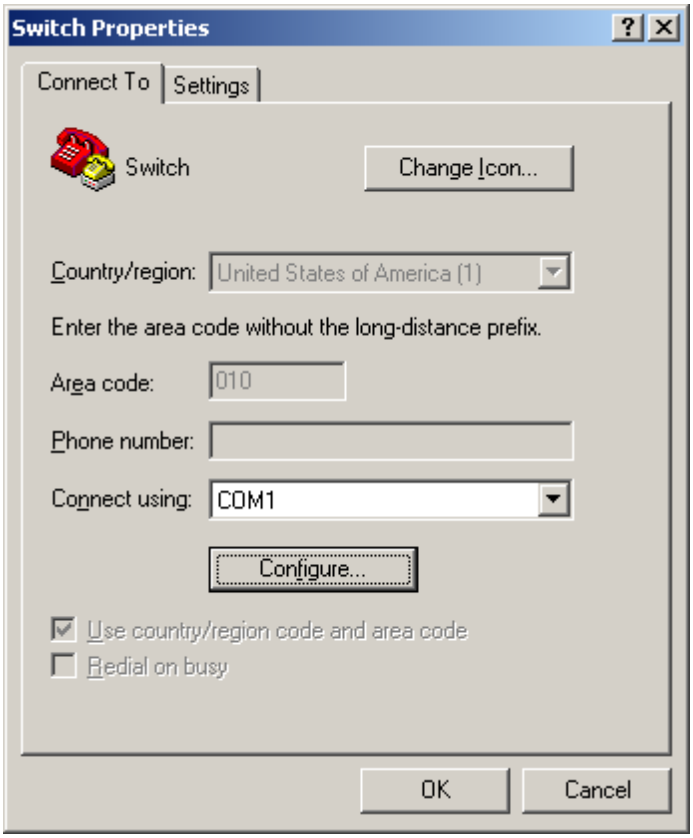
5. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



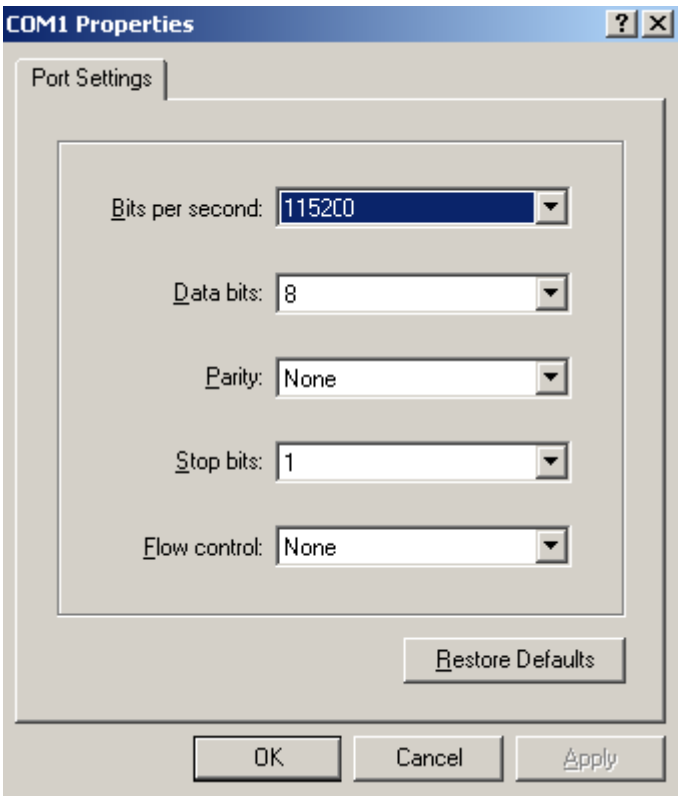
b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



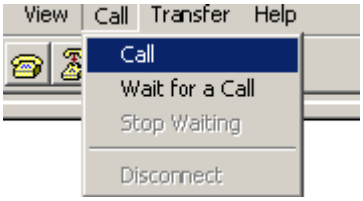
c. Select 115200 from the Bits per second list and click OK.

Figure 11 Modifying the baud rate



d. Select Call > Call to reestablish the connection.

Figure 12 Reestablishing the connection

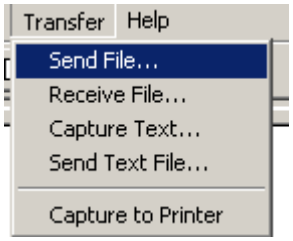


6. Press **Enter** to start downloading the file.

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

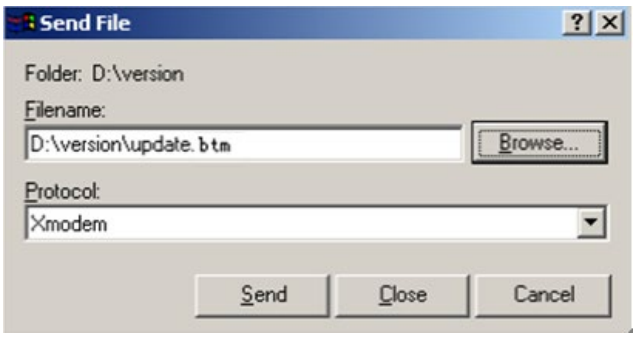
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



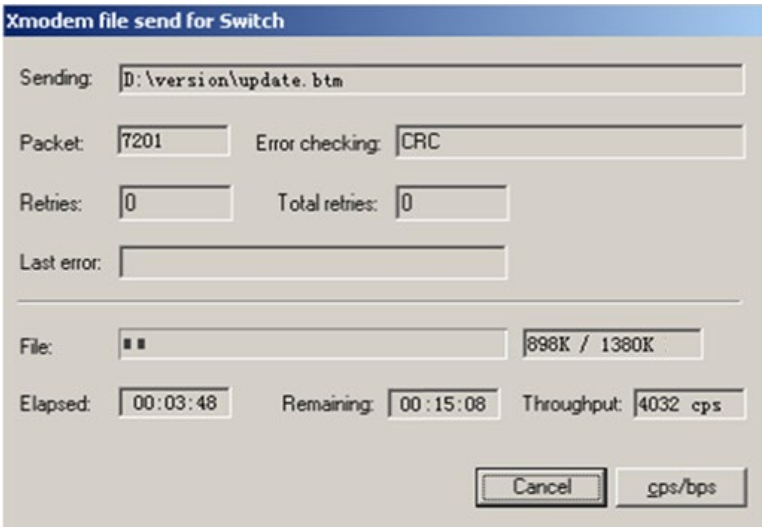
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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 ...CCCCCCCCCCCCCC  ...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

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

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.