Hewlett Packard Enterprise

HPE 1950-CMW710-R3507P09 Release Notes

Contents

List of tables

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 1950-CMW710-R3507P09. 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 1950-CMW710-R3507P09 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 3507P09

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

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
R3507P09	R3507P02	2023-02-03	Release	Fixed bugs.
R3507P02	R3507	2021-09-21	Release	Fixed bugs.
R3507	R3506P11	2021-06-08	Release	Fixed bugs. New feature • EAD assistant
R3506P11	R3506P10	2021-01-29	Release	Fixed bugs.
R3506P10	R3506P03	2020-11-12	Release	Fixed bugs.
R3506P03	R3208P16	2020-03-24	Release	Fixed bugs.
R3208P16	R3208P03	2019-03-15	Release	Fixed bugs.
R3208P03	R3115P08	2017-12-20	Release	Fixed bugs.
R3115P08	R3115P06	2017-03-20	Release	Fixed bugs.
R3115P06	R3115P03	2016-12-22	Release	Fixed bugs.
R3115P03	R3115P01	2016-09-27	Release	Fixed bugs.
R3115P01	R3115	2016-08-16	Release	Fixed bugs.
R3115	R3113P05	2016-07-15	Release	Fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R3113P05	R3113P03	2016-06-15	Release	Fixed bugs.
R3113P03	R3113P02	2016-05-27	Release	Fixed bugs.
R3113P02	R3112	2016-05-06	Release	Fixed bugs.
R3112	R3111P07	2016-03-18	Release	New feature • SSH • Configuration import and export Modified feature • Transceiver module source alarm Fixed bugs.
R3111P07	R3111P03	2016-02-03	Release	Fixed bugs.
R3111P03	R3111P02	2015-12-31	Release	New feature • Transceiver module alarm suppression Modified feature • Methods for IRF merge Fixed bugs.
R3111P02	R3110	2015-12-26	Release	Fixes bugs
R3110	R3109P16	2015-11-30	Release	New feature: • SNMP Modified feature: • Applying a QoS policy Fixed bugs.
R3109P16	R3109P14	2015-11-17	Release	Fixed bugs.
R3109P14	R3109P09	2015-10-31	Release	Fixed bugs. • HPE rebranding
R3109P09	R3109P05	2015-9-14	Release	Fixed bugs.
R3109P05	R3109P01	2015-6-16	Release	Fixed bugs.
R3109P01	R3108P02	2015-4-2	Release	New features: • RADIUS voice VLAN attribute for 802.1X and MAC authentication • 802.1X online user handshake reply Fixed bugs.
R3108P02	ESS 3107	2015-1-12	Release	Fixed bugs.
E3107	First release	2014-10-30	ESS	First release.

Hardware and software compatibility matrix

CAUTION:

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

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	1950 Switch Series
Hardware platform	HPE OfficeConnect 1950-24G-2SFP+-2XGT Switch JG960A HPE OfficeConnect 1950-48G-2SFP+-2XGT Switch JG961A HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ Switch JG962A HPE OfficeConnect 1950-48G-2SFP+-2XGT-PoE+ Switch JG963A
Minimum memory requirements	1 GB
Minimum Flash requirements	512 M
Boot ROM version	Version 147 or higher (Note: Use the summary command in any view to view the version information. Please see Note ②)
Host software	1950-CMW710-R3507P09.ipe
iMC version	iMC EAD 7.3(E0611P10) iMC QoSM 7.3(E0505P01) iMC PLAT 7.3(E0705P12) iMC UAM 7.3 (E0604P01)
iNode version	iNode PC 7.3 (E0585)
Web version	None
Remarks	None

Display the system software and Boot ROM versions of 1950:

```
<HPE>display version
HPE Comware Software, Version 7.1.070, Release 3507P09    ----- Note①
Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP
HPE 1950 48G 2SFP+ 2XGT PoE+ Switch uptime is 0 weeks, 0 days, 0 hours, 2 minute
s


Slot 1:
Uptime is 0 weeks,0 days,0 hours,2 minutes
1950-48G-2SFP+-2XGT-PoE+ JG963A with 1 Processor
BOARD TYPE:          1950-48G-2SFP+-2XGT-PoE+ JG963A
DRAM:                1024M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.B
Bootrom Version:     147                ------ Note②
CPLD 1 Version:      001
```

```
Release Version:    HPE 1950 48G 2SFP+ 2XGT PoE+ JG963A-3507P09
Patch Version  :    None
```

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 R3507P09~R3208P16

None

Hardware feature updates in R3208P03

The following cables are supported:

Product code	HPE description	Cable length
JL290A	HPE X2A0 10G SFP+ to SFP+ 7m Active Optical Cable	7 m (22.97 ft)
JL291A	HPE X2A0 10G SFP+ to SFP+ 10m Active Optical Cable	10 m (32.81 ft)
JL292A	HPE X2A0 10G SFP+ to SFP+ 20m Active Optical Cable	20 m (65.62 ft)

Hardware feature updates in R3115P08~R3115

None

Hardware feature updates in R3113P05

R3113P05 supports the following new hardware:

- Flashes that support 4-bit ECC check:
  - MICRON: MT29F4G08ABADAWP:D
  - SPANSION: S34ML01G200TFI003
- Flashes that support 8-bit ECC check:
  - MXIC: MX30LF4G28AB

Hardware feature updates in R3113P03~R3108P02

None

Hardware feature updates in E3107

First release

Software feature and command updates

For more information about the software feature and command update history, see *HPE 1950-CMW710-R3507P09 Release Notes (Software Feature Changes).*

MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
1950-CMW710-R3507P09~1950-CMW710-R3111P03			
1950-CMW710-R3111P02			
New	hh3c-port-security.mib	HH3C-PORT-SECURITY-MIB	Added descriptions and support for the following Trap: hh3cSecureAddressLearned hh3cSecureViolation hh3cSecureLoginFailure hh3cSecureLogon hh3cSecureLogoff hh3cSecureRalmLoginFailure hh3cSecureRalmLogon hh3cSecureRalmLogoff
Modified	None	None	None
1950-CMW710-R3110			
New	hh3c-splat-inf-new.mib	HH3C-LswINF-MIB	Added descriptions and support for the following MIBs: hh3cifPktBufTable
	hh3c-lsw-dev-adm.mib	HH3C-LSW-DEV-ADM-MIB	Added descriptions and support for the following MIBs: hh3cLswSlotPktBufFree hh3cLswSlotPktBufInit hh3cLswSlotPktBufMin hh3cLswSlotPktBufMiss
Modified	None	None	None

Item	MIB file	Module	Description
1950-CMW710-R3109P16~1950-CMW710-R3109P05			
New	None	None	None
Modified	None	None	None
1950-CMW710-R3109P01			
New	None	None	None
Modified	rfc1213-mib.docx	IP-MIB	ipForwarding (1.3.6.1.2.1.4.1) Only support read operation ipDefaultTTL (1.3.6.1.2.1.4.2) Only support read operation
1950-CMW710-R3108P02			
New	None	None	None
Modified	None	None	None
1950-CMW710-E3107			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R3507P09

None

Operation changes in R3507P02

- PHY chip (Ten GigabitEthernet copper port) firmware update from 1.88 to 1.89.

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

- Excluded the *freeradius.bin* file from the IPE file.

Operation changes in R3506P10

None

Operation changes in R3506P03

An SSL server policy to be used for HTTPS does not support the following cipher suites:

- Cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm MD5.
- Cipher suite that uses key exchange algorithm RSA, data encryption algorithm 128-bit RC4, and MAC algorithm SHA.
- Export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC4, and MAC algorithm MD5.
- Export cipher suite that uses key exchange algorithm RSA, data encryption algorithm RC2, and MAC algorithm MD5.
- Cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.
- Export cipher suite that uses key exchange algorithm RSA, data encryption algorithm DES_CBC, and MAC algorithm SHA.
- Cipher suite that uses key exchange algorithm RSA, data encryption algorithm 3DES_EDE_CBC, and MAC algorithm SHA.

Operation changes in R3208P16

None

Operation changes in R3208P03

- Modified the over-temperature protection feature.

  When the switching chip junction temperature exceeds 107 °C, the switch displays a log and reboots.

Operation changes in R3115P08

- The **bpdu-drop any** command in Layer 2 Ethernet interface view added support for dropping PVST and PVST+ packets.

Operation changes in R3115P06

None

Operation changes in R3115P03

None

Operation changes in R3115P01

None

Operation changes in R3115

None

Operation changes in R3113P05

None

Operation changes in R3113P03

None

Operation changes in R3113P02

None

Operation changes in R3112

None

Operation changes in R3111P07

None

Operation changes in R3111P03

Added support on Port Security logging.

Operation changes in R3111P02

None

Operation changes in R3110

None

Operation changes in R3109P16

None

Operation changes in R3109P14

None

Operation changes in R3109P09

- None

Operation changes in R3109P05

None

Operation changes in R3109P01

None

Operation changes in R3108P02

1. Change to the forwarding for packets with the destination MAC address 0180-c200-000e by default.

   Before modification, packets with the destination MAC address 0180-c200-000e are transparently forwarded by default.

   After modification, packets with the destination MAC address 0180-c200-000e are not transparently forwarded by default.
2. Deletes the autoconfiguration feature.

Operation changes in E3107

First release

Restrictions and cautions

- The offline detect timer for MAC authentication and the aging timer for dynamic MAC address entries must be set to the same value.
- 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.

Open problems and workarounds

None

List of resolved problems

Resolved problems in R3507P09

202212141432

- Symptom: A port might not come up.

- Condition: This symptom occurs if a 10-GE copper port operates at 1000 Mbps.

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.

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.

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.

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

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

202008260498

- Symptom: Port isolation does not take effect on an aggregate interface.
- Condition: This symptom might occur if port isolation is configured on an aggregate interface where multiple ACs exist.

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.

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.

202001080562

- Symptom: A MAC address cannot be learned into the corresponding VLAN.
- Condition: This symptom occurs if an IP subnet-based VLAN is configured and an interface in the VLAN receives packets with the same source MAC address.

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.

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.

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.

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.

201905080677

- Symptom: On an ADCampus network, the device obtains an incorrect automated VCF fabric deployment template.
- Condition: This symptom might occur if the device is an access node and tries to obtain an automated VCF fabric deployment template.

201904180672

- Symptom: IPv6-AH packets cannot match an ACL rule with the protocol specified as ipv6-ah.
- Condition: This symptom might occur if the protocol is specified as ipv6-ah for an ACL rule.

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.

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 R3208P16

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.

201801050451

- Symptom: The MAC information of an 802.1X user is deleted. As a result, traffic cannot be forwarded.
- Condition: This symptom occurs if an 802.1X user logs in to the subordinate member device of an IRF fabric, and then the IRF fabric splits.

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:
  - Bind more than 13 static addresses to the DHCP address pool.
  - 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.

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.

201810110329

- Symptom: A 10-GE copper port cannot work at 10 Gbps or works unstably at 10 Gbps.
- Condition: This symptom occurs if the 10-GE copper port is directly connected to another 10-GE copper port.

201810110290

- Symptom: DHCP server MIBs fail to be read.
- Condition: None.

201809140102

- Symptom: Port security configuration changes after a software upgrade.
- Condition: This symptom might occur if the port security-configured switch is upgraded to R3208P10 or R3208P12.

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.

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.

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.

201809290352

- Symptom: A 10-gigabit fiber port has CRC packet error information after receiving traffic for a long period of time.
- Condition: This symptom might occur if a 10-gigabit fiber port has been receiving traffic for a long period of time.

201810300318

- Symptom: The CPU usage of the subordinate IRF member device becomes higher gradually.
- Condition: This symptom occurs if the IRF fabric runs for a long period of time and a large number of interface up/down events occur on the subordinate device.

201812170354

- Symptom: The **display device manuinfo** command does not display power supply information.
- Condition: This symptom occurs if the **display device manuinfo** command is executed.

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.

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.

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.

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.

201807160406

- Symptom: The MAC address entry aging timer is different from the offline detect timer.
- Condition: This symptom occurs if the hit bit of the first packet with the specified MAC address is not set during MAC authentication.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

201806040605

- Symptom: The status of the LED for an interface is incorrect.
- Condition: This symptom occurs if EEE is enabled on the interface and the interface is up.

Resolved problems in R3208P03

201711030370

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

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.

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.

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.

201710260388

- Symptom: The device does not support the ACL deployed by the 802.1X authentication server.
- Condition: This symptom occurs if a rule in the deployed ACL contains the range keyword.

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.

201710260631

- Symptom: A 10 GE copper interface cannot come up.
- Condition: None.

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.

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.

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.

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 R3115P08

201703060242

- Symptom: Packet loss occurs on an edge aggregate interface if the interface has not received LACPDUs within the LACP timeout interval.
- Condition: This symptom might occur if an edge aggregate interface has not received LACPDUs within the LACP timeout interval.

201703060053

- Symptom: The switch is connected to a Cisco IP phone installed with a key expansion module. When PoE is enabled on the interface connected to the phone, the phone can be powered on, but the key expansion module cannot start.
- Condition: This symptom might occur if the following operations are performed:
  a. Connect the switch to a Cisco IP phone installed with a key expansion module.
  b. Enable PoE on the interface connected to the phone.
  c. Set the maximum power for the PoE-enabled interface.

201607280306

- Symptom: SSH connections cannot be established if no Suite B cryptographic suite is specified for SSH.
- Condition: This symptom might occur if no Suite B cryptographic suite is specified for SSH.

201606130301

- Symptom: An authentication server cannot be removed from a TACACS scheme in the Web interface.
- Condition: This symptom might occur if an authentication server is removed from a TACACS scheme in the Web interface.

201606080536

- Symptom: An AudioCodes IP phone sending CDP packets cannot be assigned to the critical voice VLAN.
- Condition: This symptom might occur if an AudioCodes IP phone sends CDP packets.

201701170366

- Symptom: The user VLAN information in user event logs is inconsistent with the authorization VLAN information that the server issues to users.
- Condition: This symptom might occur if the server issues authorization VLAN information to users that pass authentication.

201702060403

- Symptom: The1950 24G 2SFP+ 2XGT JG960A, 1950 48G 2SFP+ 2XGT JG961A, 950 24G 2SFP+ 2XGT PoE+ JG962A and 1950 48G 2SFP+ 2XGT PoE+ JG963A switch might lose software image files and configuration files.
- Condition: None.

201702130126

- Symptom: In certain conditions, an IRF fabric cannot be pinged after it reboots.
- Condition: This symptom might occur if port security is enabled on the IRF fabric, and the maximum number of secure MAC addresses allowed on a port is set to 1.

201701190157

- Symptom: In certain conditions, users cannot come online after the IRF fabric that the users access is rebooted.
- Condition: This symptom might occur if the following conditions exist:
  - Port security is enabled on the IRF fabric, and port security in **userlogin-secure** mode is enabled on the port that the users access.
  - The IRF fabric is rebooted.

201701180065

- Symptom: Multicast traffic fails to be forwarded out of an aggregate interface.
- Condition: This symptom occurs if the status of one member port in the aggregation group changes from Unselected to Selected after the device learns multicast routes. The aggregate interface is an outgoing interface of one of the multicast routes.

201701170120

- Symptom: A memory leakage occurs on the device.
- Condition: This symptom occurs if MFF in the automatic mode is enabled and then disabled repeatedly.

Resolved problems in R3115P06

201611090264

- Symptom: An SFTP user assigned the network-operator user role has access to some commands that are supposed to be inaccessible to the user role.
- Condition: This symptom occurs if the SFTP user passes either publickey or password-publickey authentication to log in to the device and is assigned the network-operator user role.

201611070270

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

201609300342

- Symptom: A memory leakage occurs in the stpd process.
- Condition: This symptom occurs if the spanning tree feature is enabled on the device and the spanning tree operating mode is changed.

201611080056

- Symptom: CVE-2016-5195
- Condition: Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping.

201611220390

- Symptom: Authentication for new portal users fails when a large number of online portal users are logging out.
- Condition: This symptom might occur if the following conditions exist:
  - The RADIUS server provides accounting services for portal users.
  - A large number of online portal users log out.

201611220420

- Symptom: An IRF fabric cannot be accessed through the console port of the master.
- Condition: This symptom might occur if an IRF fabric is accessed through the console port of the master.

201611220435

- Symptom: After a two-chassis IRF fabric is rebooted, interface indexes change and Smart Link settings are lost.
- Condition: This symptom might occur if the following operations are performed:
  a. Delete the startup.mdb and ifindex.dat files on the IRF member switches.
  b. Save the configuration and reboot the IRF fabric.
  c. When the IRF member switches are rebooting, press **Ctrl+B** to access the Boot ROM menu of one IRF member switch. The other member switch is successfully rebooted.

201612080146

- Symptom: The switch stops responding when the scripts are executed to repeatedly display memory information about the ipoe and ifmgr processes.
- Condition: This symptom might occur if the scripts are executed to repeatedly display memory information about the ipoe and ifmgr processes.

201611220280

- Symptom: After an IRF fabric is rebooted, the VPN instance information on the master is incorrect.
- Condition: This symptom might occur if the following operations are performed on an IRF fabric:
  a. Create tunnel interfaces.
  b. Reboot the IRF fabric.

201612070648

- Symptom: 802.1X users fail 802.1X authentication.
- Condition: This symptom occurs if the primary RADIUS server frequently becomes unreachable and a large number of 802.1X users frequently come online and go offline.

201609120255

- Symptom: A large number of RXLOS interruptions occur on a transceiver module, which causes a high CPU usage and then causes the device to reboot.
- Condition: This symptom occurs if the device is connected to a port of a test device through the transceiver module.

201612090524

- Symptom: In log messages, the VLAN ID of a user is not the authorization VLAN ID assigned to the user.
- Condition: This symptom might occur if a user passes access authentication and is assigned to the authorization VLAN issued by the server.

201612080309

- Symptom: The NTP server sends the switch NTP packets that have the leap flag set to 01, but the local leap indicator of the switch is 00, and the leap flag of NTP packets sent by the switch is 00.
- Condition: This symptom might occur if the following conditions exist:
  a. A PC is directly connected to the switch's management interface and is configured as an NTP client.
  b. An NTP server sends the switch NTP packets with the leap flag set to 01.

201611250474

- Symptom: The device adds two layers of VLAN tags to an untagged packet.
- Condition: This symptom might occur if the following conditions exist:
  a. Switch A and Switch B are directly connected through trunk ports. The trunk ports permit a VLAN.
  b. Configure an access port on Switch A and Switch B, and assign the access ports to the VLAN. Configure QinQ and L2PT on the access ports.
  c. Send untagged L2PT protocol packets to the access ports.

201611180294

- Symptom: A port goes down.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security on the port and configure the limit on the number of secure MAC addresses.
  b. Send packets according to the configured limit on the number of secure MAC addresses.

201611090199

- Symptom: The debugging information has extra spaces.
- Condition: This symptom might occur if the following operations are performed:
  a. A user logs in to the device by using SSH.
  b. The user enters incorrect passwords for three times.
  c. The user fails to log in and is added to the blacklist.
  d. The debugging information of the server is viewed.

201610260405

- Symptom: A user fails to log in to the device.
- Condition: This symptom might occur if the following conditions exist:
  a. The **tcp syn-cookies enable** command is executed.
  b. The Telnet client is not directly connected to the device.
  c. The user uses an IPv6 address to log in to the device by using SSH or Telnet.

201609230450

- Symptom: When a large number of IPv6 ND messages are learned and aged, traffic forwarding might fail because ARP/ND entries fail to be issued.

- Condition: This symptom might occur if a large number of IPv6 ND messages are learned and aged.

201607180428

- Symptom: IS-IS neighborship can be established. However, routing information cannot be obtained.
- Condition: This symptom might occur if the NX9000 device sends protocol packets with the MT IS TLV whose length is 2 bytes. HPE devices consider the length as invalid. As a result, the LSPs are considered as incorrect and dropped.

201603140259

- Symptom: The device operates improperly because the fast forwarding entries and sessions generated after tunnel encapsulation are incorrectly associated.
- Condition: This symptom might occur if the byte sequence is not converted for some fields in IP headers when fast forwarding entries and sessions are generated before tunnel encapsulation.

201610260323

- Symptom: The system prompts that the characters fail to be input.
- Condition: This symptom might occur if you enter special characters when configuring a description on a client running the Windows 10 operating system.

201610140261

- Symptom: CVE-2016-6304
- Condition: Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.

201610140261

- Symptom: CVE-2016-6306
- Condition: The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

201607280524

- Symptom: CVE-2016-2177
- Condition: OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.

201605090045

- Symptom: The unsupported QCN and DCBX options are configurable on the LLDP TLV configuration page of the Web interface.
- Condition: This symptom might occur if the following operations are performed:
  a. Access the device through the Web interface.
  b. On the **Network** > **LLDP** > **LLDP-TLV** page, select an interface, select 802.1TLVs QCN and DCBX, and apply the settings.

201608170166

- Symptom: After the IMC server issues the class attribute to the NAS, the RADIUS accounting requests that the NAS sends to the server do not carry the class attribute.
- Condition: This symptom might occur if the IMC server issues the class attribute to the NAS after users pass RADIUS authentication.

201610090108

- Symptom: Two users who use the same MAC address exist on the switch when certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
  a. Both MAC authentication and 802.1X authentication are performed for the users, and MAC authentication is successful.
  b. MAC move is enabled on interfaces.

201609300434

- Symptom: On an IRF fabric, OUI addresses are lost after a master/subordinate switchover.
- Condition: This symptom might occur if the following conditions exist:
  a. The number of OUI addresses reaches the upper limit on the IRF fabric.
  b. A master/subordinate switchover occurs after the configuration is saved.

201609200500

- Symptom: The following symptoms might occur when a PBR policy is configured through the Web interface:
  - On the PBR configuration page, select **Match IPv4 ACL** to enter the ACL configuration page. A user stays on the ACL configuration page after the user adds an ACL successfully.
  - A user is redirected to the Web interface home page after the user adds a PBR policy that only has next hop information because the system does not check for empty fields for PBR policy configuration.
- Condition: This symptom might occur if a PBR policy is configured through the Web interface.

201609020107

- Symptom: When the EAD assistant redirect URL is configured through the Web interface, the system displays the "configuration already exists" message even if the configuration does not exist or take effect.
- Condition: This symptom might occur if the EAD assistant redirect URL is configured through the Web interface.

201606270081

- 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.

201603140511

- Symptom: When LLDP is disabled globally, the CPU usage of the LLDP process immediately increases to 20%-30%.
- Condition: This symptom might occur if LLDP is disabled globally.

201610150081

- Symptom: When certain conations exist, an IRF fabric does not have MAC address entries for users who pass MAC authentication. As a result, the users cannot access the network.
- Condition: This symptom might occur if the following conditions exist:
  - MAC authentication is enabled on all ports of the IRF fabric.
  - A large number of users move frequently, or ports go down and come up frequently.

Resolved problems in R3115P03

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.

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.

201609070269

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

201608250027

- Symptom: The configuration of voice VLANs fails.
- Condition: This symptom occurs if voice VLANs are configured in batch in the Web interface.

Resolved problems in R3115P01

201605050154

- Symptom: After the COA issues an authorization ACL, the session-timeout timer and the offline function do not operate correctly for the authentication users.
- Condition: This symptom occurs if the switch has MAC authentication or 802.1X authentication enabled.

201607190589

- Symptom: When a port enabled with 802.1X authentication is repeatedly shut down and brought up, the 802.1X client directly connected to the port is logged off for authorization failure.
- Condition: This symptom might occur if a port enabled with 802.1X authentication is repeatedly shut down and brought up, and an 802.1X client is directly connected to the port.

201604260394

- Symptom: The short LACP timeout interval (3 seconds) is set on member ports of an aggregate interface. When the aggregate interface is down, traffic interruption lasts for 3 seconds instead of 6 seconds.
- Condition: This symptom might occur if the short LACP timeout interval (3 seconds) is set on member ports of an aggregate interface.

201605090525

- 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.

201605090525

- 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.

201605090525

- 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.

201605090525

- 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.

201605170547

- 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.

201605170547

- 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.

201605170547

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

201605170547

- 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.

201605170547

- 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.

201605170547

- 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 R3115

201606070566

- 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.

201606070566

- 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.

201606070566

- 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.

201606070566

- 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).

201606070566

- 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.

201606070566

- 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

Resolved problems in R3113P05

201605030246

- Symptom: When a PC is quickly plugged and unplugged, the switch considers the PC as online.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has both MAC authentication and 802.1X authentication enabled.
  - The PC performs MAC authentication.
  - The interface connecting to the PC has the unicast trigger or MAC authentication delay function configured.

201606010228

- Symptom: An interface cannot correctly forward multicast packets.
- Condition: This symptom occurs if both 802.1X authentication and MAC authentication are enabled on the interface and a user successfully passes MAC authentication.

201605060393

- Symptom: After a master/subordinate switchover, the VLAN configurations of interfaces are lost.
- Condition: This symptom occurs if the IRF subordinate member switch is rebooted and a master/subordinate switchover is performed.

201605170504

- Symptom: In a three-chassis IRF fabric, after the master member is powered off and subordinate member 1 becomes the new master member, the VLAN configurations of interfaces on subordinate member 2 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use three switches to build an IRF fabric in a daisy-chain topology.
  b. Power on the master member.
  c. Power on subordinate member 1 and then subordinate member 2.
  d. Save the configuration after the IRF fabric is formed.

Resolved problems in R3113P03

201604091715

- Symptom: When a 10G Base-T port is connected to a specific device model, speed autonegotiation takes 20 to 30 seconds and the negotiation result can only be 1 Gbps.
- Condition: This symptom might occur if a 10G Base-T port is connected to a specific device model.

Resolved problems in R3113P02

201604110101

- Symptom: After a period of time, PCs cannot join the 802.1X guest VLAN.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has both 802.1X authentication and MAC authentication enabled.
  - The switch connects to multiple PCs through a hub.
  - The PCs fail to pass the MAC authentication.

201605180172

- Symptom: After the switch is rebooted, the speed downgrading autonegotiation configuration is undo speed auto downgrade on an interface that is configured with the speed auto downgrade command.
- Condition: This symptom occurs if the following operations are performed

201603010580

- Symptom: The VLAN dropdown list is unavailable on the **Network** > **IPv6** > **ND** > **New Neighbor Entry** page of the Web interface.
- Condition: This symptom might occur if IPv6 neighbor entries are configured on the **Network** > **IPv6** > **ND** > **New Neighbor Entry** page of the Web interface.

201508190171

- Symptom: After the MAC address entry and ARP entry of a MAC authentication user age out, the switch cannot generate new MAC address entry and ARP entry for the user.
- Condition: This symptom might occur if the following conditions exist:
  - MAC authentication is enabled, and MAC authentication offline detection is disabled.
  - The MAC address entry and ARP entry of a MAC authentication user age out.

201507300295

- Symptom: When DHCP snooping is enabled on an IRF fabric using the ring topology, IRF member switches reboot repeatedly.
- Condition: This symptom might occur if DHCP snooping is enabled on an IRF fabric using the ring topology.

201604140100

- Symptom: MAC authentication users cannot come online if the server issues the Cisco-AVPair attribute to the switch.
- Condition: This symptom might occur if the server issues the Cisco-AVPair attribute to the switch.

201603120042

- Symptom: The switch does not respond to the security commands input by a console user.
- Condition: This symptom might occur if the following conditions exist:
  - LLDP and access authentication are enabled on the switch.
  - The intrusion protection action is set to disable on an interface, and intrusion protection is triggered because the phone connected to the interface fails authentication.

201603230420

- 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.

201603230420

- 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.

201603230420

- 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).

201603230420

- 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.

201603230420

- 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.

201603230420

- 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.

201603170138

- 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.

201603170138

- 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.

201512280388

- Symptom: 802.1X users are reauthenticated.
- Condition: This symptom occurs if the following conditions exist:
  - The keep-online feature is enabled for 802.1X users.
  - Online 802.1X users receive EAPOL-Start packets.

201602040568

- Symptom: An IP phone is reauthenticated every 30 seconds when the Web authentication server is unreachable.
- Condition: This symptom occurs if the IP phone is connected to a port enabled with 802.1X authentication and Web authentication.

201602160644

- Symptom: The ARP packets received from a peer device are not broadcasted in a VLAN.
- Condition: This symptom occurs if ARP snooping is enabled in the VLAN.

201512290192

- Symptom: CVE-2015-3194

- Condition: Fixed vulnerability which can be exploited in a DoS attack, if device is presented with a specific ASN.1 signature using the RSA.

201512290192

- Symptom: CVE-2015-3195
- Condition: Fixed vulnerability with malformed OpenSSL X509_ATTRIBUTE structure used by the PKCS#7 and CMS routines which may cause memory leak.

201512290192

- Symptom: CVE-2015-3196
- Condition: Fixed vulnerability where a race condition can occur when specific PSK identity hints are received.

201512290192

- Symptom: CVE-2015-1794
- Condition: Fixed vulnerability if a client receives a ServerKeyExchange for an anonymous Diffie-Hellman (DH) ciphersuite which can cause possible Denial of Service (DoS) attack.

Resolved problems in R3112

201601110412

- Symptom: The CPU usage of an IRF fabric is high if LLDP is enabled on a large number of up interfaces.
- Condition: This symptom might occur if LLDP is enabled for a large number of up interfaces on an IRF fabric.

201602170470

- Symptom: The add or remove DNS server IP operation fails on the **Network** > **DNS** page of the Web interface.
- Condition: This symptom might occur if a DNS server IP address is added or removed on the **Network** > **DNS** page of the Web interface.

201601270478

- Symptom: The **Resources** > **PKI** page of the Web interface stays in the loading status.
- Condition: This symptom might occur if the **Resources** > **PKI** page of the Web interface is accessed.

201601280398

- Symptom: When the Firefox browser is used to access the Web interface, the dropdown lists on some pages are unavailable.
- Condition: This symptom might occur if the Firefox browser is used to perform one of the following operations:
  - Add IPv4 static routes on the **Network** > **Static Routing** page.
  - Create a rate limit for an interface on the **QoS** > **Rate Limit** page.
  - Configure IRF port bindings on the **Device** > **IRF** page.

Resolved problems in R3111P07

201512130013

- Symptom: An interface in a VLAN mapped to an MSTI fails to be assigned to the MSTI.

- Condition: This symptom might occur if the link type of the interface is changed between trunk and access repeatedly.

201601180281

- Symptom: A Web page is incorrectly displayed. To display the correct page, you must refresh the page.
- Condition: This symptom occurs if you access the **Device**, **Network**, or **QoS** page first through Web and then access other pages.

201512230197

- Symptom: The PoE status is incorrectly displayed for an interface.
- Condition: This symptom occurs if you access the PoE configuration page of a PoE switch through Web.

201511160443

- Symptom: During 802.1X authentication that uses the EAP method, the RADIUS packets exchanged in one user authentication process might be sent to different servers.
- Condition: This symptom occurs if RADIUS server load sharing is enabled on the switch.

201507310169

- Symptom: The subordinate IRF member switch might reboot unexpectedly.
- Condition: This symptom might occur if patches are repeatedly installed and removed in an IRF fabric.

Resolved problems in R3111P03

201511300121

- Symptom: The switch acting as an NTP client cannot be synchronized to an NTP server.
- Condition: This symptom occurs if the NTP server is a Cisco device.

201510300354

- Symptom: A user goes offline immediately after the user comes online through 802.1X authentication.
- Condition: This symptom occurs if the following conditions exist:
  - Another user comes online through MAC authentication before the 802.1X user.
  - The 802.1X user is assigned the same VLAN as the MAC-authenticated user.

201512090334

- Symptom: The operation of backing up the configuration file fails.
- Condition: This symptom occurs if the following conditions exist:
  - The MIB node hh3cCfgOperateServerAddress is configured to specify the file backup server.
  - The IP address of the file backup server is in the range of x.x.x.224 to x.x.x.255.

201511190408

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

201511190408

- Symptom: CVE-2015-7704

- Condition: An ntpd client forged by a DDoS attacker located anywhere on the Internet, that 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.

201511190408

- 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.

201511190408

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

201501160412

- Symptom: The switch cannot send trap messages if it is rebooted after SNMP is configured. The switch can send trap messages correctly if it is rebooted again.
- Condition: This symptom might occur if the following operations have been performed:
  - Configure SNMP.
  - Save the configuration and reboot the switch.
  - Enter the CLI and do not execute any commands.

201511230171

- Symptom: The CPU occupied by the aclmgrd process is not released. As a result, the CPU usage of the switch is high.
- Condition: This symptom occurs if master/subordinate switchover occurs in an IRF fabric.

Resolved problems in R3111P02

201512040456

- Symptom: A subordinate switch in an IRF fabric reboots repeatedly.
- Condition: This symptom occurs if the .mdb file is deleted and the IRF fabric is power cycled.

201511190389

- Symptom: The CPU usage of an IRF fabric is high.
- Condition: This symptom occurs if the following conditions exist:
  - A VLAN interface on the IRF fabric is configured with an IP address.
  - A member switch in the IRF fabric is configured as a DHCP server.

201512200032

- Symptom: On an IRF fabric enabled with 802.1X or MAC authentication, the CPU usage is high on the member switches that do not reboot after an active/standby MPU switchover occurs.
- Condition: This symptom might occur if 802.1X or MAC authentication is configured on the IRF fabric, and an active/standby MPU switchover occurs.

201512170385

- Symptom: The Dashboard page of the Web interface displays incorrect device type information.
- Condition: This symptom might occur if the Web interface is used to log in to the switch.

Resolved problems in R3110

201510280475

- Symptom: A user goes offline immediately after the user comes online through 802.1X authentication.
- Condition: This symptom occurs if the switch uses a RADIUS scheme and local accounting for 802.1X authentication.

201511180069

- Symptom: The first 24 ports on a 52-port switch cannot communicate with the last 24 ports on the switch.
- Condition: This symptom might occur if the switch is rebooted repeatedly.

Resolved problems in R3109P16

201507160220

- Symptom: CVE-2014-8176
- Condition: If a DTLS peer receives application data between the ChangeCipherSpec and Finished messages. May result in a segmentation fault or potentially, memory corruption.

201507160220

- Symptom:CVE-2015-1788
- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

201507160220

- Symptom: CVE-2015-1789
- Condition: X509_cmp_time does not properly check the length of the ASN1_TIME string and/or accepts an arbitrary number of fractional seconds in the time string. An attacker can use this to craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS on applications that verify certificates or CRLs.

201507160220

- Symptom: CVE-2015-1790
- Condition: The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201507160220

- Symptom: CVE-2015-1791
- Condition: If a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket then a race condition can occur potentially leading to a double free of the ticket data.

201507160220

- Symptom: CVE-2015-1792
- Condition: When verifying a signedData message the CMS code can enter an infinite loop. This can be used to perform denial of service against any system which verifies signedData messages using the CMS code.

Resolved problems in R3109P14

201504130201

- Symptom: After successful 802.1X authentication, a port sets the tagging status to untagged for packets of a voice VLAN. As a result, IP phones receive untagged packets.
- Condition: This symptom might occur if the following conditions exist:
  - 802.1X authentication and voice VLAN are configured on the port.
  - The device-traffic-class=voice attribute is configured on the authentication server.

201509020039

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

201509160335

- Symptom: User authentication fails.
- Conditions: This symptom occurs if the PEAP authentication method is used to perform 802.1X authentication.

201509110280

- Symptom: The switch performs 802.1X reauthentication when it receives an EAPOL-Start message from a Windows client. After several reauthentication failures, the Windows client is put in silent state, and its NIC becomes unavailable.
- Condition: This symptom might occur if the following conditions exist:
  - 802.1X authentication and voice VLAN are configured on the switch.
  - The authentication server is unreachable, and the Windows client is in the 802.1X critical VLAN.

201509260060

- Symptom: The Web interface is slow in refreshing webpages or does not respond when PoE is configured for an IRF fabric.
- Condition: This symptom might occur if the Web interface is used to configure PoE for an IRF fabric.

201510130396

- Symptom: Some services might operate incorrectly or the switch might reboot unexpectedly.
- Condition: This symptom occurs when a MIB management tool is used to obtain the power supply information of the switch.

Resolved problems in R3109P09

201509010289

- Symptom: The switch logs out a MAC-authenticated user that sends packets to the switch before the offline detect timer expires.
- Condition: This symptom might occur if MAC authentication is configured.

201508080233

- Symptom: The switch cannot start up.
- Condition: This symptom occurs if the switch's flash memory is corrupted.

201508310155

- Symptom: An interface advertises an Auto-negotiation TLV with an incorrect value and fails to negotiate with the peer interface.
- Condition: This symptom occurs when LLDP is enabled globally and on the interface.

201506180249

- Symptom: CVE-2015-3143
- Description: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request.

201506180249

- Symptom: CVE-2015-3148
- Description: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

201506100324

- Symptom: Software upgrade fails for an IRF fabric from the Web interface.
- Conditions: This symptom might occur when you upgrade software for the IRF fabric from the Web interface.

201503050138

- Symptom: The flash memory of an IRF subordinate device is not available after the device reboots to rejoin the IRF fabric.
- Conditions: This symptom might occur if you have saved running configuration only for this subordinate device in the IRF fabric before you reboot the device.

201504090194

- Symptoms: CVE-2015-0209
- Condition: A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources.

201504090194

- Symptoms: CVE-2015-0286
- Condition: DoS vulnerability in certificate verification operation. Any application which performs certificate verification is vulnerable including OpenSSL clients and servers which enable client authentication.

201504090194

- Symptoms: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

201504090194

- Symptoms:CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.

201504090194

- Symptoms: CVE-2015-0289

- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201505150249

- Symptom: TCP processing errors occur during an NQA operation. The operation fails, and services are interrupted on the switch.
- Condition: This symptom might occur if an NQA operation is performed on the switch.

201504200256

- Symptom: The switch cannot provide DHCP services correctly as a DHCP server.
- Condition: This symptom might occur if the following conditions exist:
  - A DHCP client has obtained an IP address from the DHCP server, and its address lease expires.
  - The client is configured as a BOOTP client.

201505240024

- Symptom: Some PoE registers restore the default values after the PoE firmware is online updated.
- Condition: This symptom might occur if a PoE firmware online update is performed.

201506170069

- Symptom: An 802.1X client is forced to log off soon after it logs in.
- Condition: This symptom occurs if the 802.1X authentication server assigns security policies such as ACL and user profile to the client after the client passes the 802.1X authentication.

Resolved problems in R3109P05

201505150457

- Symptom: A PoE switch cannot supply power over PoE to IP phones of some vendors.
- Condition: This symptom occurs when you connect the IP phones to the switch and supply power over PoE.

201506130010

- Symptom: A port is brought up and can forward packets when the MDIX mode negotiation fails.
- Condition: This symptom occurs if the following operations have been performed:
  - Use a straight-through cable to connect the port and its peer port.
  - Configure the same MDI (or MDIX) mode at both ends of the cable.

201504020079

- Symptom: The Web interface is stuck at the **Please wait…** window when you upgrade system software in the Web interface.
- Condition: This symptom occurs after you select the upgrade file and click **Apply** in the Web interface.

201502110444

- Symptom: The switch reconnects to the SDN controller immediately after an unexpected disconnection from the controller.
- Condition: This symptom might occur if an active/standby MPU switchover occurs when the controller is issuing a large number of flow table entries to the switch.

201506100226

- Symptom: The port connected to an IP phone is removed from the voice VLAN after both the LLDP aging timer and the voice VLAN aging timer expire.
- Condition: This symptom might occur if the switch establishes a neighbor relationship with the IP phone and advertises voice VLAN information to the IP phone through LLDP.

201505110287

- Symptom: A user passes MAC authentication, but the authentication server fails to assign the authorization VLAN to the user.
- Condition: This symptom occurs if the VLAN attribute issued by the authentication server in the Access-Accept packet ends with **\0x00**.

201505270138

- Symptom: The switch cannot use IP subnet-based VLANs to match and forward untagged packets.
- Condition: This symptom might occur if IP subnet-based VLANs are configured on the switch.

201412120103

- Symptom: After a reboot, the IDs of some members in an IRF fabric are changed to the default number 1. The affected members cannot rejoin the IRF fabric.
- Condition: This symptom might occur if operations are frequently performed on the NOR flash memory, for example, save the configuration file frequently.

201505110140

- Symptom: The switch reboots unexpectedly or cannot provide services correctly when a MAC address move occurs.
- Condition: This symptom might occur if one of the following conditions exists on the switch:
  - 100 or more ARP entries in a VLAN have the same MAC address, and the MAC address moves between ports.
  - The MAC address of an ARP entry moves between ports five times per second or more frequently.

Resolved problems in R3109P01

201501290379

- Symptom: 802.1X users fail to log in.
- Condition: This symptom occurs if the authorization VLANs assigned by the authentication server use a format incompatible with the switch.

201412150089

- Symptom: Portal users log out unexpectedly.
- Condition: This symptom occurs if the following conditions exist:
  - DHCP and portal roaming are enabled.
  - The portal users roam between APs by using mobile devices.

201503020204

- Symptom: A PoE switch cannot supply power correctly.
- Condition: This symptom occurs if the PoE module receives incorrect instructions.

201501210272

- Symptom: CVE-2014-3569
- Condition: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling.

201501210272

- Symptom: CVE-2014-3571
- Condition: A carefully crafted DTLS message can cause a segmentation fault in OpenSSL due to a NULL pointer dereference. This could lead to a Denial Of Service attack.

201501210272

- Symptom: CVE-2015-0206
- Condition: A memory leak can occur in the dtls1_buffer_record function under certain conditions. In particular this could occur if an attacker sent repeated DTLS records with the same sequence number but for the next epoch. The memory leak could be exploited by an attacker in a Denial of Service attack through memory exhaustion.

201501210272

- Symptom: CVE-2015-0205
- Condition: An OpenSSL server will accept a DH certificate for client authentication without the certificate verify message. This effectively allows a client to authenticate without the use of a private key. This only affects servers which trust a client certificate authority which issues certificates containing DH keys.

201501210272

- Symptom: CVE-2014-3570
- Condition: Bignum squaring (BN_sqr) may produce incorrect results on some platforms, including x86_64. This bug occurs at random with a very low probability, and is not known to be exploitable in any way.

201501210272

- Symptom: CVE-2015-0204
- Condition: An OpenSSL client will accept the use of an RSA temporary key in a non-export RSA key exchange ciphersuite. A server could present a weak temporary key and downgrade the security of the session.

201501210272

- Symptom: CVE-2014-3572
- Condition: An OpenSSL client will accept a handshake using an ephemeral ECDH ciphersuite using an ECDSA certificate if the server key exchange message is omitted. This effectively removes forward secrecy from the ciphersuite.

201501210272

- Symptom: CVE-2014-8275
- Condition: By modifying the contents of the signature algorithm or the encoding of the signature, it is possible to change the certificate's fingerprint. Only custom applications that rely on the uniqueness of the fingerprint may be affected.

Resolved problems in R3108P02

201411140514

- Symptom: The IRF member ID configuration might fail to take effect.
- Condition: This symptom can be seen when you modify the IRF member ID of a switch.

201412120040

- Symptom: CVE-2014-3567
- Condition: When an OpenSSL SSL/TLS/DTLS server receives a session ticket the integrity of that ticket is first verified. In the event of a session ticket integrity check failing, OpenSSL will fail to free memory causing a memory leak. By sending a large number of invalid session tickets an attacker could exploit this issue in a Denial of Service attack.

201412120040

- Symptom: SSL 3.0 Fallback protection
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

201501070257

- Symptom: An HP switch cannot use CDP-compatible LLDP to exchange information with a Cisco device.
- Condition: This symptom occurs when the following conditions exist:
  - The HP switch is directly connected to a Cisco device.
  - The HP switch is enabled with LLDP.
  - The Cisco device is enabled with CDP.

201407160505

- Symptom: The message showing that "Transceiver type and port configuration mismatched!" appears.
- Condition: This symptom occurs when a 1000-Mbps transceiver module is installed and removed repeatedly.

Resolved problems in E3107

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 1950 Switch Series Getting Started Guide
- HPE 1950 Switch Series User Guid

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 OfficeConnect 1950 Switch Series Getting Started Guide

Software features

Table 4 Software features of the 1950 series

Feature	HPE OfficeConnect 1950-24G-2SFP+-2XGT Switch	HPE OfficeConnect 1950-48G-2SFP+-2XGT Switch	HPE OfficeConnect 1950-24G-2SFP+-2XGT-PoE+ Switch	HPE OfficeConnect 1950-48G-2SFP+-2XGT-PoE+ Switch
Full duplex Wire speed L2 switching capacity	128 Gbps	176 Gbps	128 Gbps	176 Gbps
Whole system Wire speed L2 switching Packet forwarding rate	95.232 Mpps	130.952 Mpps	95.232 Mpps	130.952 Mpps
Forwarding mode	Store-forward			
IRF	• Ring topology • Daisy chain topology • IRF comprised of different models			
Link aggregation	• Aggregation of 10-GE ports • Aggregation of GE ports • Static link aggregation • Dynamic link aggregation • Inter-device aggregation • A maximum of 14 aggregation groups on a device • A maximum of 128 inter-device aggregation groups • A maximum of 8 ports for each aggregation group			
Flow control	• IEEE 802.3x flow control • Back pressure			
Jumbo Frame	• Supports maximum frame size of 9000			
MAC address table	• 16K MAC addresses • 1K static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port			

VLAN	• Port-based VLANs (4094 VLANs)
ARP	• 256 entries • 64 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)
ND	• 256 entries • 64 static entries
VLAN virtual interface	8
DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server
DNS	• Static DNS • Dynamic DNS • IPv4 and IPv6 DNS
IPv4 unicast route	• 64 static routes • Policy-based routing
IPv6 unicast route	• 32 static routes
Multicast	• IGMP snooping • MLD snooping
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 • 16 PVST instances
QoS/ACL	• Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4) • Eight output queues for each port • SP/WRR/SP+WRR queue scheduling algorithms • Port-based rate limiting • Flow-based redirection • Time range
Mirroring	• Stream mirroring • Port mirroring • Multiple mirror observing port
Remote mirroring	• Port remote mirroring (RSPAN)
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication

	• 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 • Trunk port authentication • Dynamic 802.1X-based QoS/ACL/VLAN assignment
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • IMC NMS • System log • Hierarchical alarms • NTP • Power supply alarm function • Fan and temperature alarms
Maintenance	• Ping and Tracert • Remote maintenance through Telnet

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"

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.

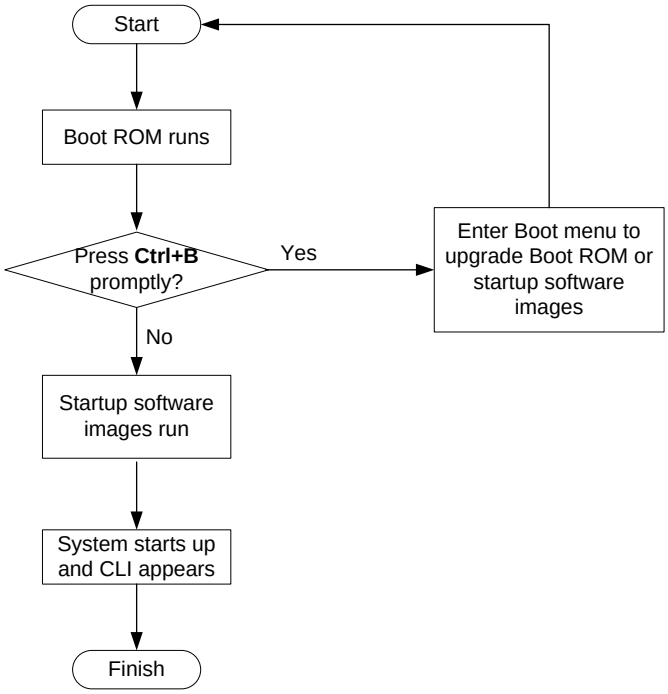
  The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

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, 1950-CMW710-BOOT-R3113P02.bin and 1950-CMW710-SYSTEM-R3113P02.bin.

Upgrading from the CLI

Loading Software Using TFTP

You can remotely download Boot ROM and system software images from a TFTP server at the CLI as follows.

Step 1: Configure an IP address for the switch

```
<HPE>ipsetup ip-address 100.1.1.12 24
```

Step 2: Download the system software image file from the TFTP server.

```
<HPE>upgrade 100.1.1.10 runtime file 1950.ipe
The file flash:/1950.ipe already exists.Overwrite?[Y/N]y
Verifying server file...
Downloading file 1950.ipe from remote TFTP server, please wait...
...Done.
Verifying the file flash:/1950.ipe on slot 1......Done.
HPE 1950-48G-2SFP+-2XGT images in IPE:
  1950-cmw710-boot-r3109p05.bin
  1950-cmw710-system-r3109p05.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/1950-cmw710-boot-r3109p05.bin already exists on slot 1.
File flash:/1950-cmw710-system-r3109p05.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file 1950-cmw710-boot-r3109p05.bin to flash:/1950-cmw710-boot-r3109p05.b
in..........Done.
Decompressing file 1950-cmw710-system-r3109p05.bin to
flash:/1950-cmw710-system-r3109p05.bin.....................................
..........Done.
Verifying the file flash:/1950-cmw710-boot-r3109p05.bin on slot 1...Done.
Verifying the file flash:/1950-cmw710-system-r3109p05.bin on slot 1.....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.
Decompression completed.
Do you want to delete flash:/1950.ipe now? [Y/N]:y
```

Step 3: Download and load the Boot ROM file.

```
<HPE>upgrade 100.1.1.10 bootrom 1950-cmw710-boot-r3109p05.bin
Verifying server file...
Downloading file 1950-cmw710-boot-r3109p05.bin from remote TFTP server, please
 wait.....................................................................Done.
This command will upgrade the Boot ROM file on the specified board(s), Continue?
 [Y/N]:y
Now upgrading the Boot ROM of slot 1, please wait...
.......Done.
```

Step 4: Reboot the device to validate the new system software.

```
<HPE> reboot
```

Note that if flash memory is insufficient, load the Boot ROM image first and delete useless files to free up Flash memory before you load the system software 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**—38,400
   - **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 5.

Table 5 Minimum free storage space requirements

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.
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 1950-24G-2SFP+-2XGT Switch BOOTROM, Version 143            *
*                                                                              *
********************************************************************************
Copyright (c) 2010-2016 Hewlett-Packard Development Company, L.P.

Creation Date       : Dec  2 2016, 14:00:56
CPU Clock Speed     : 400MHz
Memory Size         : 1024MB
Flash Size          : 512MB
CPLD Version        : 001
PCB Version         : Ver.B
Mac Address         : 00e0fc035100

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

Press one of the shortcut key combinations at prompt.

Table 6 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 112                          *
*                                                                              *
********************************************************************************

   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 7 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 8).

Table 8 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 9). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 1950 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 9 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 10.

Table 10 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 11 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 12 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 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.

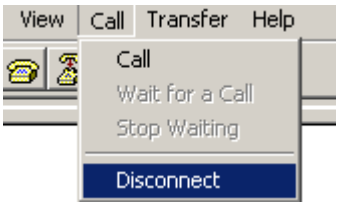
```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
```

```
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 38400bps as the download rate for the console port, skip this task.

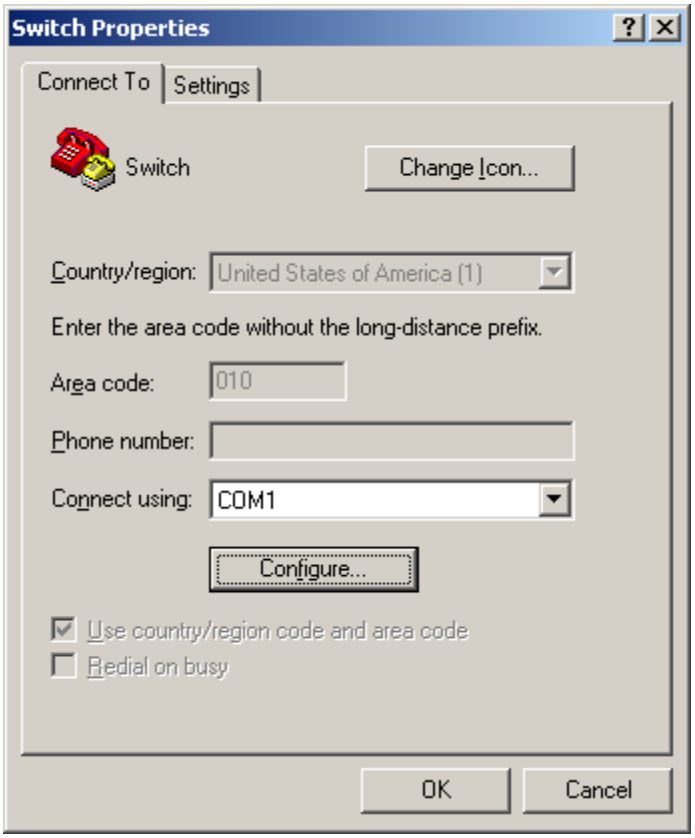
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



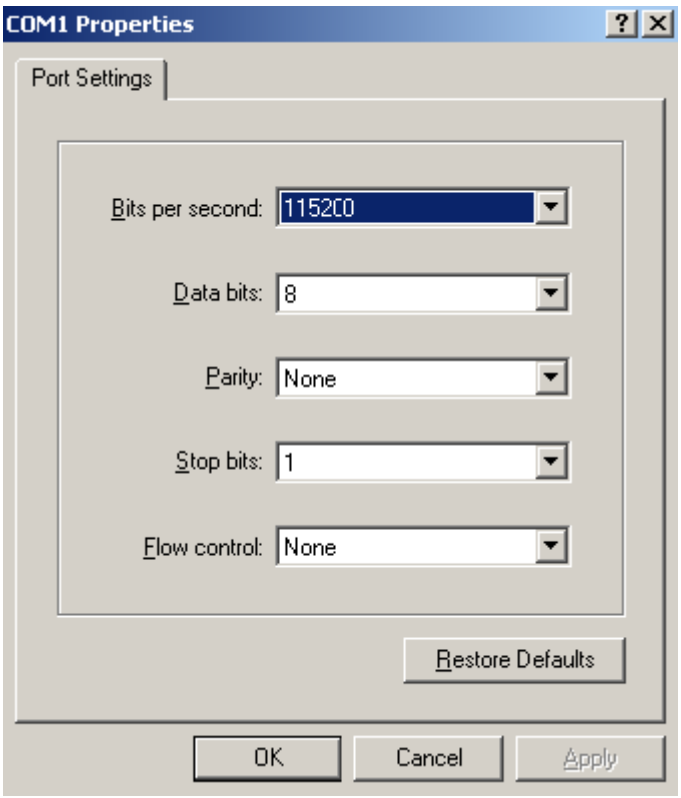
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



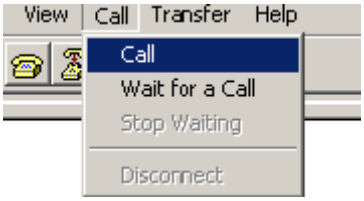
   c. Select **115200** from the **Bits per second** list and click **OK**.

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:

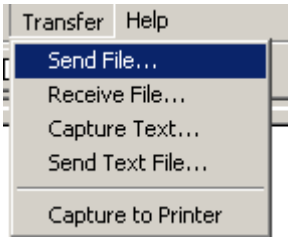
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

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
```

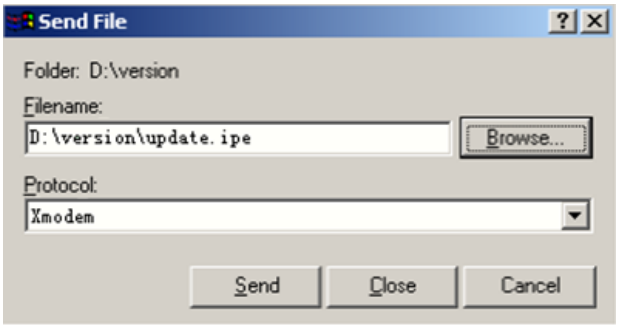
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 6 Transfer menu



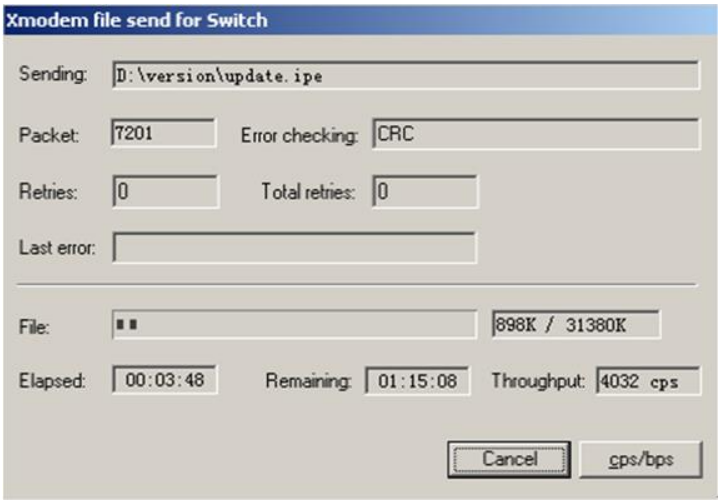
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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 38400 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 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 38400bps, restore it to 38400bps as described in step 5.a. If the baud rate is 38400bps, skip this step.

NOTE:

The console port rate reverts to 38400bps 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 13 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 14 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.

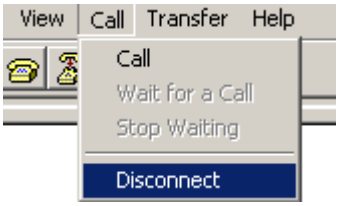
```
Please select your download baudrate:
1.  9600
2.  19200
3.* 38400
4.  57600
5.  115200
0.  Return to boot menu

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
```

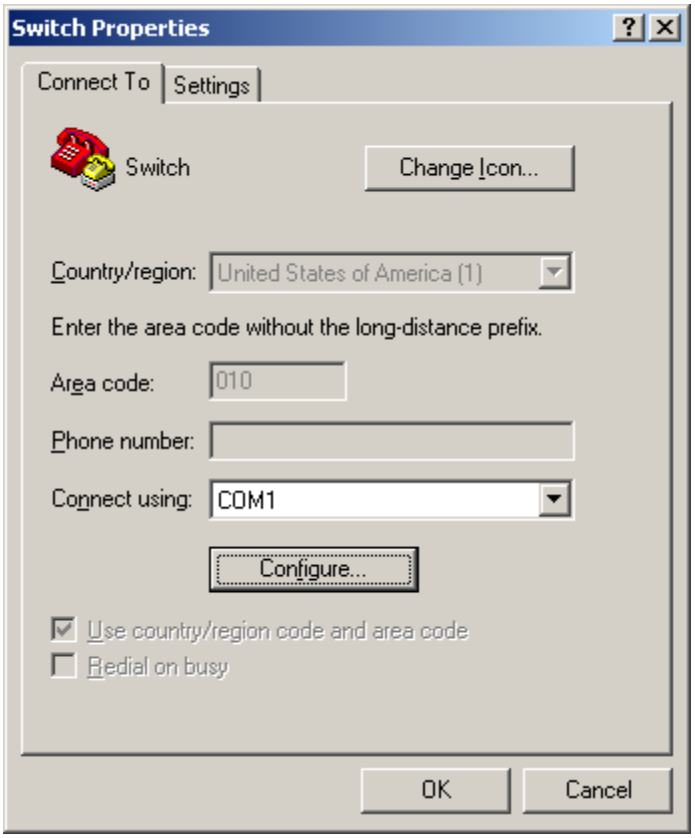
5. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 38400bps as the download rate for the console port, skip this task.
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



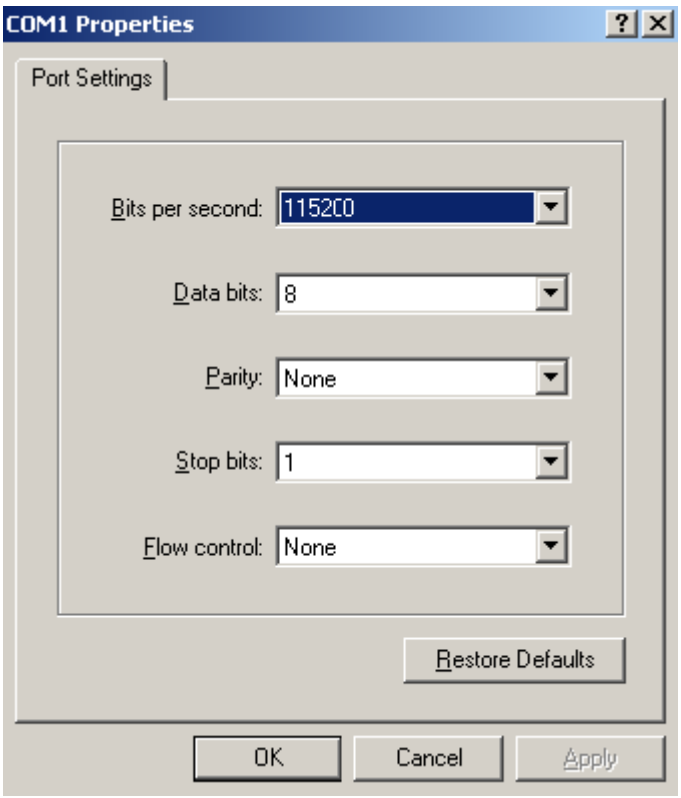
b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



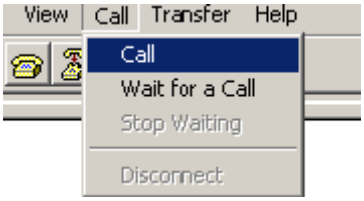
c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



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

Figure 12 Reestablishing the connection

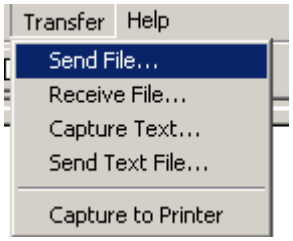


6. Press **Enter** to start downloading the file.

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

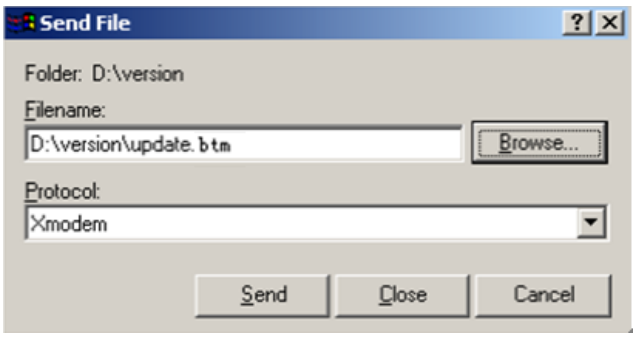
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



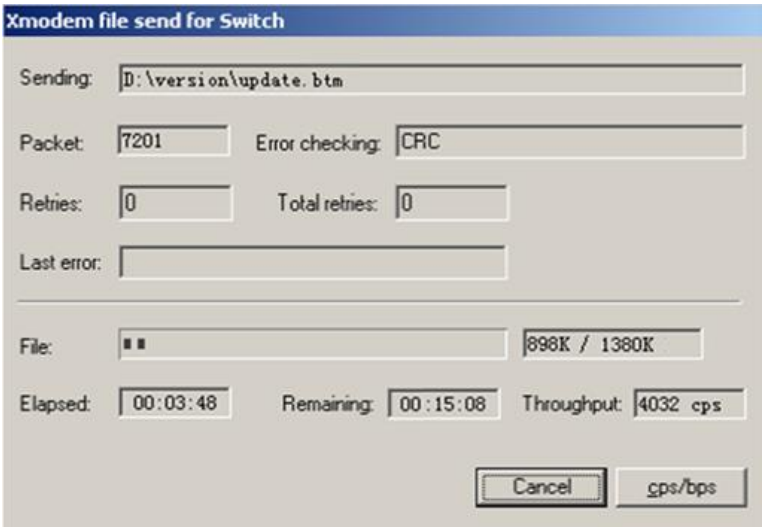
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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 38400bps, restore it to 38400bps at the prompt, as described in step 4.a. If the baud rate is 38400bps, skip this step.

```
Please change the terminal's baudrate to 38400 bps, press ENTER when ready.
```

NOTE:

The console port rate reverts to 38400bps 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.

Hewlett Packard Enterprise

HPE 1950-CMW710-R3507P09
Release Notes
Software Feature Changes

Contents

Release 3507P09

This release has no feature changes.

Release 3507P02

This release has no feature changes.

Release 3507

This release has the following changes:

- Modified feature: EAD assistant

Modified feature: EAD assistant

Feature change description

As from this version, you can use both EAD assistant and MAC authentication on the device.

Before modification: EAD assistant is mutually exclusive with MAC authentication and port security.

- You cannot enable EAD assistant when MAC authentication or port security is enabled globally.
- You cannot enable MAC authentication or port security globally when EAD assistant is enabled.

After modification: EAD assistant is still mutually exclusive with the port security feature, but you can use both EAD assistant and MAC authentication on the device. When you use both EAD assistant and MAC authentication on the device, follow these restrictions and guidelines:

- If both EAD assistant and MAC authentication are configured on the device, the MAC address of a user that fails MAC authentication is not marked as a silent MAC address. If the user has never passed MAC authentication, packets from the user can trigger MAC authentication again only after the user's EAD entry ages out.
- As a best practice, do not configure MAC authentication guest VLANs or critical VALNs. The VLANs might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- As a best practice, do not configure the Web authentication or IP source guard feature. The feature might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- If the MAC address of a user has been marked as a silent MAC address before EAD assistant is enabled, packets from the user can trigger 802.1X or MAC authentication only after the quiet timer expires.

Command changes

None.

Release 3506P10

This release has no feature changes.

Release 3506P03

This release has no feature changes.

Release 3208P16

This release has no feature changes.

Release 3208P03

This release has no feature changes.

Release 3116P05

This release has no feature changes.

Release 3116

This release has no feature changes.

Release 3115P08

This release has no feature changes.

Release 3115P06

This release has no feature changes.

Release 3115P03

This release has no feature changes.

Release 3115P01

This release has no feature changes.

Release 3115

This release has no feature changes.

Release 3113P05

This release has no feature changes.

Release 3113P03

This release has no feature changes.

Release 3113P02

This release has no feature changes.

Release 3112

This release has the following changes:

- New feature: SSH
- New feature: Configuration import and export
- Modified feature: Transceiver module source alarm

New feature: SSH

Overview

Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.

SSH uses the typical client-server model to establish a channel for secure data transfer based on TCP.

The device can act as an SSH server and provide the following services for SSH clients:

- Secure Telnet-Stelnet provides secure and reliable network terminal access services.
- Secure FTP-SFTP uses SSH connections to provide secure file transfer based on SSH2.
- Secure Copy-SCP offers a secure method to copy files based on SSH2.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 provides better performance and security than SSH1. In non-FIPS mode, the device that acts as an SSH server supports both SSH2 and SSH1. In FIPS mode, it supports only SSH2.

When the device acts as an SSH server, it supports using local password authentication to examine the validity of the username and password of an SSH client. After the SSH client passes the authentication, the two parties establish a session for data exchange.

Generic SSH server configuration procedure

When the device acts as an SSH server, perform the following tasks on the device:

- Generate local DSA or RSA key pairs.
- Enable the Stelnet, SFTP, or SCP server function.
- Configure a local user, and assign the user role network-admin and authorize the SSH service to the user.

Restrictions and guidelines

When you configure the device as an SSH server, follow these restrictions and guidelines:

- To support SSH clients that use different types of key pairs, generate both DSA and RSA key pairs on the SSH server.
- SSH supports only locally generated DSA and RSA key pairs with default names.
- The key modulus length must be less than 2048 bits when you generate the DSA key pair on the SSH server.
- The attributes (such as user role or FTP directory) that are assigned to the SSH user depend on the local user configuration on the SSH server.

- All SSH clients can initiate SSH connections to the device when any one of the following conditions exists:
  - You do not specify any ACLs.
  - The specified ACL does not exist.
  - The specified ACL does not have any rules.
- When acting as an SFTP server, the device does not support SFTP connections initiated by SSH1 clients.

New feature: Configuration import and export

This feature allows you to import or export configuration as follows:

- Export the running configuration to a configuration file on the current host.
- Import a configuration file on the current host and specify the configuration file as the next-startup configuration file. You can choose to overwrite the running configuration with the settings in the specified configuration file or not.

Modified feature: Transceiver module source alarm

Feature change description

The default status of the transceiver module source alarm feature changed from enabled to disabled.

Command changes

Modified command: transceiver phony-alarm-disable

Syntax

transceiver phony-alarm-disable

Views

User view

Change description

Before modification: Transceiver module source alarm is enabled by default.

After modification: Transceiver module source alarm is disabled by default.

Release 3111P07

This release has no feature changes.

Release 3111P03

New feature: Transceiver module source alarm

Disabling transceiver module source alarm

If you install a transceiver module whose vendor name is not **HPE**, the system repeatedly outputs traps and log messages to notify you to replace the module. If the transceiver module is manufactured or customized by HPE, you can disable transceiver module source alarm so the system stops outputting traps and log messages.

Command reference

Use **transceiver phony-alarm-disable** to disable transceiver module source alarm.

Use **undo transceiver phony-alarm-disable** to restore the default.

transceiver phony-alarm-disable

Syntax

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Default

Transceiver module source alarm is enabled.

Views

User view

Predefined user roles

network-admin

Usage guidelines

If you install a transceiver module whose vendor name is not **HPE**, the system repeatedly outputs traps and log messages to notify you to replace the module. If the transceiver module is manufactured or customized by HPE, you can disable transceiver module source alarm so the system stops outputting traps and log messages.

Examples

Disable transceiver module source alarm.

```
<Sysname> transceiver phony-alarm-disable
```

Modified feature: Methods for IRF merge

Feature change description

Before modification: To complete IRF merge, manually reboot the device after the IRF port binding operation.

After modification:

Use one of the following methods to complete IRF merge:

- Click Active IRF Port Configuration. The device automatically reboots to join the IRF fabric.
- Manually reboot the device.

Command changes

N/A

Release 3111P02

This release has no feature changes.

Release 3110

This release has the following changes:

- New feature: SNMP
- Modified feature: Applying a QoS policy

New feature: SNMP

Overview

Simple Network Management Protocol (SNMP) is an Internet standard protocol widely used for a network management station (NMS) to access and manage the devices (agents) on a network. After you enable SNMP on the device, the device acts as an SNMP agent.

SNMP enables an NMS to read and set the values of the variables on an agent. The agent sends traps to report events to the NMS.

MIB

Management Information Base (MIB) is a collection of objects. It defines hierarchical relations between objects and object properties, including object name, access privilege, and data type.

An NMS manages a device by reading and setting the values of variables (for example, interface status and CPU usage) on the device. These variables are objects in the MIB.

OID and subtree

A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a dotted numeric string that uniquely identifies the path from the root node to a leaf node. For example, the object **internet** is uniquely identified by the OID {1.3.6.1}.

A subtree is like a branch in the tree hierarchy. It contains a root node and the lower-level nodes of the root node. A subtree is identified by the OID of the root node.

MIB view

A MIB view is a subset of a MIB. You can control NMS access to MIB objects by specifying a MIB view for the username or community name that the NMS uses. For a subtree included in a MIB view, all nodes in the subtree are accessible to the NMS. For a subtree excluded in a MIB view, all nodes in the subtree are inaccessible to the NMS.

Subtree mask

A subtree mask is in hexadecimal format. It identifies a MIB view collectively with the subtree OID.

To determine whether an MIB object is in a MIB view, convert the subnet mask to binary bits (0 and 1) and match each bit with each node number of the object OID from left to right. If the 1-bit corresponded node numbers of the object OID are the same as those of the subtree OID, the MIB object is in the MIB view. The 0-bit corresponded node numbers can be different from those of the subtree OID.

For example, the view determined by the subtree OID 1.3.6.1.6.1.2.1 and the subtree mask 0xDB (11011011 in binary) includes all the nodes under the subtree OID 1.3.*.1.6.*.2.1, where * represents any number.

NOTE:

- If the number of bits in the subtree mask is greater than the number of nodes of the OID, the excessive bits

of the subtree mask will be ignored during subtree mask-OID matching.

- If the number of bits in the subtree mask is smaller than the number of nodes of the OID, the short bits of the subtree mask will be set to 1 during subtree mask-OID matching.
- If no subtree mask is specified, the default subtree mask (all ones) will be used for mask-OID matching.

SNMP versions

You can enable SNMPv1, SNMPv2c, or SNMPv3 on a device. For an NMS and an agent to communicate, they must run the same SNMP version.

- SNMPv1 and SNMPv2c use community name for authentication. An NMS can access a device only when the NMS and the device use the same community name.
- SNMPv3 uses username for authentication and allows you to configure an authentication key and a privacy key to enhance communication security. The authentication key authenticates the validity of the packet sender. The privacy key is used to encrypt the packets transmitted between the NMS and the device.

SNMP access control

SNMPv1 and SNMPv2 access control

SNMPv1 and SNMPv2 uses community name for authentication. To control NMS access to MIB objects, configure one or both of the following settings on the community name that the NMS uses:

- Specify a MIB view for the community. You can specify only one MIB view for a community.
  - If you grant read-only permission to the community, the NMS can only read the values of the objects in the MIB view.
  - If you grant read-write permission to the community, the NMS can read and set the values of the objects in the MIB view.
- Specify a basic IPv4 ACL or a basic IPv6 ACL for the community to filter illegitimate NMSs from accessing the agent.
  - Only NMSs with the IPv4/IPv6 address permitted in the IPv4/IPv6 ACL can access the SNMP agent.
  - If you do not specify an ACL, or the specified ACL does not exist, all NMSs in the SNMP community can access the SNMP agent. If the specified ACL does not have any rules, no NMS in the SNMP community can access the SNMP agent.

SNMPv3 access control

SNMPv3 uses username for authentication. To control NMS access to MIB objects, configure one or both of the following settings on the username that the NMS uses:

- Create an SNMPv3 group and assign the username to the group. The user has the same access right as the group.

  When you create the group, specify one or more MIB views for the group. The MIB views include read-only MIB view, read-write MIB view, or notify MIB view. You can specify only one MIB view of a type for a group.
  - Read-only MIB view only allows the group to read the values of the objects in the view.
  - Read-write MIB view allows the group to read and set the values of the object in the view.
  - Notify MIB view automatically sends a notification to the NMS when the group accesses the view.
- Specify a basic IPv4 ACL or a basic IPv6 ACL for the user and group, respectively, to filter illegitimate NMSs. Only the NMSs permitted by the ACLs for both the user and group can access the SNMP agent. The following rules apply to the ACLs for the user and group:

- If you do not specify an ACL, the specified ACL does not exist, or the specified ACL does not have any rules, all NMSs that use the username can access the SNMP agent.
- If you have specified an ACL and the ACL has rules, only the NMSs permitted by the ACL can access the agent.

Restrictions and guidelines

An NMS and an agent must use the same SNMP version for communication. If you configure multiple SMNP versions for an agent and NMS, they will negotiate for a version to use.

Modified feature: Applying a QoS policy

Feature change description

On the Web interface, a QoS policy cannot be applied in the outbound direction.

Command changes

N/A

Release 3109P16

This release has no feature changes.

Release 3109P14

This release has no feature changes.

Release 3109P09

This release has no feature changes.

Release 3109P05

This release has the following changes:

New feature: Upgrading PSE firmware in service

New feature: Upgrading PSE firmware in service

Upgrading PSE firmware in service

You can upgrade the PSE firmware in service in either of the following modes:

- **Refresh mode**—Updates the PSE firmware without deleting it. You can use the refresh mode in most cases.
- **Full mode**—Deletes the current PSE firmware and reloads a new one. Use the full mode if the PSE firmware is damaged and you cannot execute any PoE commands.

Command reference

display poe pse

Use **display poe pse** to display PSE information.

Syntax

display poe pse [*pse-id*]

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

pse-id: Specifies a PSE by its ID.

Usage guidelines

If you do not specify a PSE, this command displays information about all PSEs.

Examples

Display detailed information about PSE 7.

```
<Sysname> display poe pse 7
 PSE ID                              : 7
 Slot No.                           : 1
 SSlot No.                          : 0
 PSE Model                          : LSP7POEB
 PSE Status                         : Enabled
 Power Priority                     : Low
 Current Power                      : 0.0      W
 Average Power                      : 0.0      W
 Peak Power                         : 0.0      W
```

```
Max Power                          : 370.0    W
Remaining Guaranteed Power       : 370.0    W
PSE CPLD Version                   : -
PSE Software Version              : 130
PSE Hardware Version              : 57633
Legacy PD Detection               : Disabled
Power Utilization Threshold      : 80
PD Power Policy                    : Disabled
PD Disconnect-Detection Mode     : AC
```

Table 1 Command output

Field	Description
PSE ID	ID of the PSE.
Slot No.	Slot number of the PSE.
SSlot No.	Subslot number of the PSE.
PSE Status	PoE status of the PSE.
Power Priority	Power priority of the PSE.
Current Power	Current power of the PSE.
Average Power	Average power of the PSE.
Peak Power	Peak power of the PSE.
Max Power	Maximum power of the PSE.
Remaining Guaranteed Power	Remaining guaranteed power of the PSE = Maximum guaranteed power of the PSE – Total maximum power of all critical PIs of the PSE.
PSE CPLD Version	PSE CPLD version number.
PSE Software Version	PSE software version number.
PSE Hardware Version	PSE hardware version number.
Legacy PD Detection	Nonstandard PD detection status: • **Enabled**. • **Disabled**.
Power Utilization Threshold	PSE power alarm threshold.
PD Power Policy	PD power management policy mode.
PD Disconnect Detection Mode	PD disconnection detection mode.

poe update

Use **poe update** to upgrade a PSE firmware when the device is operating.

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

Views

User view

Predefined user roles

network-admin

Parameters

full: Upgrades the PSE firmware in full mode.

refresh: Upgrades the PSE firmware in refresh mode.

filename: Specifies the name of the upgrade file, a case-sensitive string of 1 to 64 characters. The specified file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

You can upgrade the PSE firmware in service in either of the following modes:

- **Refresh mode**—Updates the PSE firmware without deleting it. You can use the refresh mode in most cases.
- **Full mode**—Deletes the current PSE firmware and reloads a new one. Use the full mode if the PSE firmware is damaged and you cannot execute any PoE commands.

Examples

Upgrade the firmware of PSE 7 in service.

```
<Sysname> poe update refresh POE-168.bin pse 7
```

Release 3109P01

This release has no feature changes.

Release 3108P02

This release has no feature changes.

ESS 3107

First release.