|  |
| --- |
|  |
| HPE 5130EI-CMW710-R3507P10 Release Notes |
|  |
|  |
|  |
| The information in this document is subject to change without notice.  © Copyright 2015,2023 Hewlett Packard Enterprise Development LP |

Contents

[Introduction 1](#_Toc129617054)

[Version information 1](#_Toc129617055)

[Version number 1](#_Toc129617056)

[Version history 1](#_Toc129617057)

[Hardware and software compatibility matrix 8](#_Toc129617058)

[Upgrade restrictions and guidelines 10](#_Toc129617059)

[Hardware feature updates 10](#_Toc129617060)

[Hardware feature updates in R3507P10~R3115 10](#_Toc129617061)

[Hardware feature updates in R3113P05 10](#_Toc129617062)

[Hardware feature updates in R3113P03~R3108P03 10](#_Toc129617063)

[Hardware feature updates in R3108P01 10](#_Toc129617064)

[Hardware feature updates in R3106P01 10](#_Toc129617065)

[Hardware feature updates in R3106 10](#_Toc129617066)

[Software feature and command updates 11](#_Toc129617067)

[MIB updates 11](#_Toc129617068)

[Operation changes 12](#_Toc129617069)

[Operation changes in R3507P10 12](#_Toc129617070)

[Operation changes in R3507P09 12](#_Toc129617071)

[Operation changes in R3507P02 12](#_Toc129617072)

[Operation changes in R3507 13](#_Toc129617073)

[Operation changes in R3506P11 13](#_Toc129617074)

[Operation changes in R3506P10 13](#_Toc129617075)

[Operation changes in R3506P08 13](#_Toc129617076)

[Operation changes in R3506P06 13](#_Toc129617077)

[Operation changes in R3506P02 13](#_Toc129617078)

[Operation changes in R3506 14](#_Toc129617079)

[Operation changes in R3208P16 14](#_Toc129617080)

[Operation changes in R3208P15 14](#_Toc129617081)

[Operation changes in R3208P12 14](#_Toc129617082)

[Operation changes in R3208P10 14](#_Toc129617083)

[Operation changes in R3208P08 14](#_Toc129617084)

[Operation changes in R3208P03 14](#_Toc129617085)

[Operation changes in R3208 14](#_Toc129617086)

[Operation changes in R3207 15](#_Toc129617087)

[Operation changes in R3115P08 15](#_Toc129617088)

[Operation changes in R3115P07 15](#_Toc129617089)

[Operation changes in R3115P06 15](#_Toc129617090)

[Operation changes in R3115P05 15](#_Toc129617091)

[Operation changes in R3115P03 15](#_Toc129617092)

[Operation changes in R3115P01 15](#_Toc129617093)

[Operation changes in R3115 15](#_Toc129617094)

[Operation changes in R3113P05 15](#_Toc129617095)

[Operation changes in R3113P03 15](#_Toc129617096)

[Operation changes in R3113P02 16](#_Toc129617097)

[Operation changes in R3112 16](#_Toc129617098)

[Operation changes in R3111P07 16](#_Toc129617099)

[Operation changes in R3111P03 16](#_Toc129617100)

[Operation changes in R3111P02 16](#_Toc129617101)

[Operation changes in R3111P01 16](#_Toc129617102)

[Operation changes in R3110 16](#_Toc129617103)

[Operation changes in R3109P16 16](#_Toc129617104)

[Operation changes in R3109P14 16](#_Toc129617105)

[Operation changes in R3109P09 16](#_Toc129617106)

[Operation changes in R3109P07 16](#_Toc129617107)

[Operation changes in R3109P05 17](#_Toc129617108)

[Operation changes in R3109P04 17](#_Toc129617109)

[Operation changes in R3109P03 17](#_Toc129617110)

[Operation changes in R3109P01 17](#_Toc129617111)

[Operation changes in R3108P03 17](#_Toc129617112)

[Operation changes in R3108P01 17](#_Toc129617113)

[Operation changes in R3106P01 17](#_Toc129617114)

[Operation changes in R3106 17](#_Toc129617115)

[Restrictions and cautions 17](#_Toc129617116)

[Open problems and workarounds 18](#_Toc129617117)

[List of resolved problems 18](#_Toc129617118)

[Resolved problems in R3507P10 18](#_Toc129617119)

[Resolved problems in R3507P09 18](#_Toc129617120)

[Resolved problems in R3507P02 19](#_Toc129617121)

[Resolved problems in R3507 21](#_Toc129617122)

[Resolved problems in R3506P11 22](#_Toc129617123)

[Resolved problems in R3506P10 22](#_Toc129617124)

[Resolved problems in R3506P08 23](#_Toc129617125)

[Resolved problems in R3506P06 23](#_Toc129617126)

[Resolved problems in R3506P02 24](#_Toc129617127)

[Resolved problems in R3506 24](#_Toc129617128)

[Resolved problems in R3208P16 25](#_Toc129617129)

[Resolved problems in R3208P15 26](#_Toc129617130)

[Resolved problems in R3208P12 28](#_Toc129617131)

[Resolved problems in R3208P10 30](#_Toc129617132)

[Resolved problems in R3208P08 32](#_Toc129617133)

[Resolved problems in R3208P03 38](#_Toc129617134)

[Resolved problems in R3208 42](#_Toc129617135)

[Resolved problems in R3207 42](#_Toc129617136)

[Resolved problems in R3115P08 42](#_Toc129617137)

[Resolved problems in R3115P07 43](#_Toc129617138)

[Resolved problems in R3115P06 45](#_Toc129617139)

[Resolved problems in R3115P05 49](#_Toc129617140)

[Resolved problems in R3115P03 50](#_Toc129617141)

[Resolved problems in R3115P01 51](#_Toc129617142)

[Resolved problems in R3115 53](#_Toc129617143)

[Resolved problems in R3113P05 54](#_Toc129617144)

[Resolved problems in R3113P03 55](#_Toc129617145)

[Resolved problems in R3113P02 55](#_Toc129617146)

[Resolved problems in R3112 58](#_Toc129617147)

[Resolved problems in R3111P07 59](#_Toc129617148)

[Resolved problems in R3111P03 59](#_Toc129617149)

[Resolved problems in R3111P02 61](#_Toc129617150)

[Resolved problems in R3111P01 61](#_Toc129617151)

[Resolved problems in R3110 61](#_Toc129617152)

[Resolved problems in R3109P16 62](#_Toc129617153)

[Resolved problems in R3109P14 63](#_Toc129617154)

[Resolved problems in R3109P09 63](#_Toc129617155)

[Resolved problems in R3109P07 64](#_Toc129617156)

[Resolved problems in R3109P05 66](#_Toc129617157)

[Resolved problems in R3109P04 67](#_Toc129617158)

[Resolved problems in R3109P03 67](#_Toc129617159)

[Resolved problems in R3109P01 68](#_Toc129617160)

[Resolved problems in R3108P03 69](#_Toc129617161)

[Resolved problems in R3108P01 71](#_Toc129617162)

[Resolved problems in R3106P01 72](#_Toc129617163)

[Resolved problems in R3106 72](#_Toc129617164)

[Support and other resources 72](#_Toc129617165)

[Accessing Hewlett Packard Enterprise Support 72](#_Toc129617166)

[Documents 73](#_Toc129617167)

[Related documents 73](#_Toc129617168)

[Documentation feedback 73](#_Toc129617169)

[Appendix A Feature list 74](#_Toc129617170)

[Hardware features 74](#_Toc129617171)

[Software features 74](#_Toc129617172)

[Appendix B Fixed security vulnerabilities 78](#_Toc129617173)

[Fixed security vulnerabilities in R3507P09 78](#_Toc129617174)

[Appendix C Upgrading software 79](#_Toc129617175)

[System software file types 79](#_Toc129617176)

[System startup process 79](#_Toc129617177)

[Upgrade methods 80](#_Toc129617178)

[Upgrading from the CLI 81](#_Toc129617179)

[Preparing for the upgrade 81](#_Toc129617180)

[Downloading software images to the master switch 82](#_Toc129617181)

[Upgrading the software images 84](#_Toc129617182)

[Upgrading from the Boot menu 86](#_Toc129617183)

[Prerequisites 86](#_Toc129617184)

[Accessing the Boot menu 87](#_Toc129617185)

[Accessing the basic Boot menu 88](#_Toc129617186)

[Accessing the extended Boot menu 89](#_Toc129617187)

[Upgrading Comware images from the Boot menu 90](#_Toc129617188)

[Upgrading Boot ROM from the Boot menu 98](#_Toc129617189)

[Managing files from the Boot menu 105](#_Toc129617190)

[Handling software upgrade failures 108](#_Toc129617191)

List of tables

[Table 1 Version history 1](#_Toc129617192)

[Table 2 Hardware and software compatibility matrix 8](#_Toc129617193)

[Table 3 MIB updates 11](#_Toc129617194)

[Table 4 Software features of the 5130 EI series 74](#_Toc129617195)

[Table 5 Minimum free storage space requirements 86](#_Toc129617196)

[Table 6 Shortcut keys 87](#_Toc129617197)

[Table 7 Basic Boot ROM menu options 88](#_Toc129617198)

[Table 8 BASIC ASSISTANT menu options 89](#_Toc129617199)

[Table 9 Extended Boot ROM menu options 90](#_Toc129617200)

[Table 10 EXTENDED ASSISTANT menu options 90](#_Toc129617201)

[Table 11 TFTP parameter description 91](#_Toc129617202)

[Table 12 FTP parameter description 93](#_Toc129617203)

[Table 13 TFTP parameter description 99](#_Toc129617204)

[Table 14 FTP parameter description 100](#_Toc129617205)

# Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE 5130EI-CMW710-R3507P10. 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 5130EI-CMW710-R3507P10 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

# Version information

## Version number

HPE Comware Software, Version 7.1.070, Release 3507P10

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

## Version history

|  |  |
| --- | --- |
| IMPORTANT | 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. |

* + - * 1. Version history

| Version number | Last version | Release Date | Release type | Remarks |
| --- | --- | --- | --- | --- |
| R3507P10 | R3507P09 | 2023-03-09 | Release | This version fixed bugs |
| R3507P09 | R3507P02 | 2023-02-03 | Release | This version fixed bugs. |
| R3507P02 | R3507 | 2021-09-29 | Release | This version fixed bugs. |
| R3507 | R3506P11 | 2021-06-08 | Release | This version fixed bugs and introduced feature changes.  New features include:   * + - * EAD assistant |
| R3506P11 | R3506P10 | 2021-01-29 | Release | This version fixed bugs. |
| R3506P10 | R3506P08 | 2020-11-12 | Release | This version fixed bugs and introduced feature changes.  New features include:   * + - * Configuring the 802.1p priority for control packets sent by a device       * Packet spoofing logging and filtering entry logging for SAVI       * Configuring password control over weak passwords       * Enabling password change prompt logging   Fixed bugs. |
| R3506P08 | R3506P06 | 2020-07-27 | Release | This version fixed bugs. |
| R3506P06 | R3506P02 | 2020-06-19 | Release | This version fixed bugs and introduced feature changes.  New features include:   * + - * Enabling recording untrusted DHCP servers on a DHCP snooping device   There are also modified features.  Fixed bugs. |
| R3506P02 | R3506 | 2019-12-23 | Release | This version fixed bugs. |
| R3506 | R3208P16 | 2019-07-12 | Release | This version fixed bugs and introduced feature changes.  New features include:   * + - * For more information about the new features, see *HPE 5130EI-CMW710-R3506 Release Notes (Software Feature Changes)*   There are also modified features.  Fixed bugs. |
| R3208P16 | R3208P15 | 2019-03-15 | Release | This version fixed bugs and introduced feature changes.  New features include:   * + - * Setting the block timer for MAC addresses in the blocked MAC address list       * Logging off 802.1X users       * Logging off MAC authentication users   Fixed bugs. |
| R3208P15 | R3208P12 | 2018-12-26 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * Configuring zero-to-two VLAN mapping       * Specifying DNS server information in RA messages       * Specifying DNS suffix information in RA messages       * Suppressing advertising DNS information in RA messages       * HTTP redirect       * ERPS   There are also modified features.  Fixed bugs. |
| R3208P12 | R3208P10 | 2018-09-26 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * PD detection mode   There are also modified features.  Fixed bugs. |
| R3208P10 | R3208P08 | 2018-08-29 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * Automatic obtaining of the login username for temporary user role authorization       * 802.1X EAP-TLS fragmentation for packets sent to the server       * Enabling interface consistency check for ARP and MAC address entries       * 802.1X offline detection       * Enabling SAVI and setting the entry deletion delay by using commands   There are also modified features.   * + - * Fixed bugs. |
| R3208P08 | R3208P03 | 2018-05-22 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * Shutting down an interface by OpenFlow   There are also modified features.   * + - * Fixed bugs. |
| R3208P03 | R3208 | 2017-12-20 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * VRRP   There are also modified features. |
| R3208 | R3207 | 2017-08-15 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * MAC address information display for 802.1X users in 802.1X VLANs of a specific type       * Authorization CAR action in an ISP domain       * 802.1X client   There are also modified features. |
| R3207 | R3115P08 | 2017-04-27 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * Fundamentals features       * IRF features       * Layer 2-LAN switching features   There are also modified features.  Fixed bugs. |
| R3115P08 | R3115P07 | 2017-03-20 | Release version | This version fixed bugs and introduced feature changes.  New features include:   * + - * ISP domain for users assigned to nonexistent domains   Fixed bugs. |
| R3115P07 | R3115P06 | 2017-02-16 | Release version | Modified feature:   * + - * The login success message for 802.1X users       * The login failure message for 802.1X users   Fixed bugs. |
| R3115P06 | R3115P05 | 2016-12-22 | Release version | New feature:   * + - * 802.1X MAC address binding   Modified feature:   * + - * Password configuration for MAC authentication MAC-based user accounts       * Setting the fixed-area ratio for a queue       * Setting the maximum shared-area ratio for a queue       * Setting the total shared-area ratio       * Burst feature   Fixed bugs. |
| R3115P05 | R3115P03 | 2016-10-24 | Release version | Modified feature   * + - * Operating information collection       * Maximum length of jumbo frames allowed by an Ethernet interface       * Controlling SSH client access to the SSH server       * Debugging switches   Fixed bugs. |
| R3115P03 | R3115P01 | 2016-09-27 | Release version | Modified feature   * + - * Configuring a test profile for RADIUS server status detection       * NTP support for ACL   Fixed bugs. |
| R3115P01 | R3115 | 2016-08-16 | Release version | New feature   * + - * Configuring traffic policing for all incoming traffic by using the non-MQC approach       * Bandwidth guaranteeing group       * Ignoring the ingress ports of ARP packets during user validity check   Modified feature  Fixed bugs. |
| R3115 | R3113P05 | 2016-07-15 | Release version | New features   * + - * Including user IP addresses in realtime accounting packets for MAC authentication users with dynamic IP addresses       * Configuring periodic MAC reauthentication   Modified feature:   * + - * Kernel thread deadloop detection   Fixed bugs. |
| R3113P05 | R3113P03 | 2016-06-15 | Release version | New features   * + - * PD detection mode   Fixed bugs. |
| R3113P03 | R3113P02 | 2016-05-27 | Release version | Fixed bugs. |
| R3113P02 | R3112 | 2016-05-06 | Release version | New features   * + - * Automatic negotiation for speed downgrading       * RADIUS stop-accounting packet buffering       * HWTACACS stop-accounting packet buffering       * Support of 802.1X for redirect URL assignment       * Support of MAC authentication for redirect URL assignment       * Support of port security for redirect URL assignment in specific modes       * SAVI   Modified feature   * + - * CDP compatibility for LLDP   Fixed bugs. |
| R3112 | R3111P07 | 2016-03-18 | Release version | Modified feature   * + - * Displaying the number of online 802.1X users       * Displaying the number of online MAC authentication users       * Displaying the number of online Web authentication users   Fixed bugs. |
| R3111P07 | R3111P03 | 2016-02-03 | Release version | New feature   * + - * Enabling bridging on an Ethernet interface       * Sending EAP-Success packets to 802.1X users in critical VLAN       * Triple authentication       * Enabling SNMP notifications for port security       * Enabling SNMP notifications for RRPP   Modified feature   * + - * Configuring the HTTPS listening port number for the local portal Web server       * Specifying ECDSA algorithms with different public key lengths       * Fixed bugs. |
| R3111P03 | R3111P02 | 2015-12-31 | Release version | New feature   * + - * Web authentication       * Allowing link aggregation member ports to be in the deployed flow tables       * Transceiver module alarm suppression   Modified feature   * + - * 802.1X guest VLAN assignment delay   Fixed bugs. |
| R3111P02 | R3111P01 | 2015-12-28 | Release version | Fixed bugs. |
| R3111P01 | R3110 | 2015-12-18 | Release version | Fixed bugs. |
| R3110 | R3109P16 | 2015-11-30 | Release version | New features:   * + - * Enabling SNMP notifications for new-root election and topology change events       * IP address pool authorization by AAA       * Port-specific 802.1X periodic reauthentication timer       * Manual reauthentication for all online 802.1X users on a port       * IPsec support for Suite B       * SSH support for Suite B       * Public key management support for Suite B       * PKI support for Suite B       * SSL support for Suite B   Modified feature:   * + - * FIPS self-tests       * Configuring the CDP-compatible operating mode for LLDP   Fixed bugs. |
| R3109P16 | R3109P14 | 2015-11-17 | Release version | New features:   * + - * Packet Capture   Fixed bugs. |
| R3109P14 | R3109P09 | 2015-10-31 | Release version | New features:   * + - * Including client IP addresses in realtime accounting packets for 802.1X clients with dynamic IP addresses       * Enabling MAC authentication multi-VLAN mode on a port       * RADIUS DAE server       * RADIUS server status detection       * RADIUS server load sharing       * 802.1X guest VLAN assignment delay       * Sending 802.1X protocol packets without VLAN tags       * 802.1X critical voice VLAN       * MAC authentication critical voice VLAN       * Parallel processing of MAC authentication and 802.1X authentication       * RA guard logging feature       * Displaying RA guard statistics       * Clearing RA guard statistics       * Configuring log suppression for a module   Modified features:   * + - * 802.1X command output       * MAC authentication command output       * Displaying interface information       * Configuring the types of advertisable LLDP TLVs on a port       * Specifying RADIUS servers       * Configuring SSH access control   Removed features:   * + - * Enabling PoE for a PSE       * Fixed bugs.       * HPE rebranding |
| R3109P09 | R3109P07 | 2015-9-14 | Release version | New features:   * + - * L2PT   Fixed bugs. |
| R3109P07 | R3109P05 | 2015-7-31 | Release version | New features:   * + - * MAC authentication offline detection   Fixed bugs. |
| R3109P05 | R3109P04 | 2015-6-16 | Release version | Fixed bugs. |
| R3109P04 | R3109P03 | 2015-5-28 | Release version | Fixed bugs. |
| R3109P03 | R3109P01 | 2015-5-15 | Release version | New features:   * + - * RA Guard   Modified feature: Configuring the TCP maximum segment size (MSS)  Fixed bugs. |
| R3109P01 | R3108P03 | 2015-4-2 | Release version | New features:   * + - * RADIUS voice VLAN attribute for 802.1X and MAC authentication       * 802.1X online user handshake reply   Modified feature:   * + - * Specifying startup images   Fixed bugs. |
| R3108P03 | R3108P01 | 2015-2-13 | Release version | New features:   * + - * Disabling SSL 3.0       * Login delay       * ND Snooping   Fixed bugs. |
| R3108P01 | R3106 | 2014-12-12 | Release version | Fixed bugs. |
| R3106P01 | R3106 | 2014-8-9 | Release version | Add new hardware support |
| R3106 | First release | 2014-7-28 | Release version | First release |

## Hardware and software compatibility matrix

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

* + - * 1. Hardware and software compatibility matrix

| Item | Specifications |
| --- | --- |
| Product family | 5130 EI Series |
| Hardware platform | HPE 5130-24G-4SFP+ EI Switch JG932A  HPE 5130-24G-SFP-4SFP+ EI Switch JG933A  HPE 5130-48G-4SFP+ EI Switch JG934A  HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch JG936A  HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch JG937A  HPE 5130-24G-2SFP+-2XGT EI Switch JG938A  HPE 5130-48G-2SFP+-2XGT EI Switch JG939A  HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch JG940A  HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch JG941A  HPE 5130-24G-4SFP+ EI Brazil Switch JG975A  HPE 5130-48G-4SFP+ EI Brazil Switch JG976A  HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A  HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A |
| Minimum memory requirements | 1 GB |
| Minimum Flash requirements | 512 M |
| Boot ROM version | Version 147 or higher (Note: Use the display version command in any view to view the version information. Please see Note➁) |
| Host software | 5130EI-CMW710-R3507P10.ipe |
| iMC version | iMC BIMS 7.3(E0506H01)  iMC EAD 7.3(E0611P10)  iMC QoSM 7.3(E0505P01)  iMC EIA 7.3(E0611P13)  iMC PLAT 7.3(E0705P12)  iMC NTA 7.3(E0707L06)  iMC SHM 7.3(E0707L06) |
| iNode version | iNode PC 7.3(E0585) |
| Web version | None |
| Remarks | None |

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

<Sysname>display version

HPE Comware Software, Version 7.1.070, Release 3507P10 ------ Note➀

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

HPE 5130 24G 4SFP+ EI Switch uptime is 0 weeks, 0 days, 0 hours, 3 minutes

Last reboot reason : User reboot

Boot image: flash:/5130ei-cmw710-boot-r3507p10.bin

Boot image version: 7.1.070, Release 3507P10

Compiled Sep 15 2021 11:00:00

System image: flash:/5130ei-cmw710-system-r3507p10.bin

System image version: 7.1.070, Release 3507P10

Compiled Sep 15 2021 11:00:00

Slot 2:

Uptime is 0 weeks,0 days,0 hours,3 minutes

5130-24G-4SFP+ EI with 1 Processor

BOARD TYPE: 5130-24G-4SFP+ EI

DRAM: 1024M bytes

FLASH: 512M bytes

PCB 1 Version: VER.B

Bootrom Version: 147 ------ Note➁

CPLD 1 Version: 001

Release Version: HPE 5130 24G 4SFP+ EI JG932A-3507P10

Patch Version : None

Reboot Cause : UserReboot

[SubSlot 0] 24GE+4SFP Plus

## 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 R3507P10~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~R3108P03

None

## Hardware feature updates in R3108P01

Added support for HP 5130-24G-2SFP+-2XGT EI Switch JG938A,HP 5130-48G-2SFP+-2XGT EI Switch JG939A,HP 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch JG940A,HP 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch JG941A.

## Hardware feature updates in R3106P01

Added support for HP 5130-24G-4SFP+ EI Brazil Switch JG975A,HP 5130-48G-4SFP+ EI Brazil Switch JG976A,HP 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A,HP 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A.

## Hardware feature updates in R3106

* First release.

# Software feature and command updates

For more information about the software feature and command update history, see *HPE 5130EI-CMW710-R3507P02 Release Notes (Software Feature Changes).*

# MIB updates

* + - * 1. MIB updates

| Item | MIB file | Module | Description |
| --- | --- | --- | --- |
| 5130EI-CMW710-R3507P10~5130EI-CMW710-R3506P11 | | | |
| New | None | None | None |
| Modified | None | None | None |
| 5130EI-CMW710-R3506P10 | | | |
| New | savi.mib | SAVI-MIB | Added the following objects to SaviObjectsSystemEntry:  saviObjectsSystemNotifySpoofing used for setting or obtaining the status of packet spoofing logging.  saviObjectsSystemNotifyFilter used for setting or obtaining the status of filtering entry logging.  saviObjectsSystemNotifySpoofingInterval used for setting or obtaining the log output interval for packet spoofing logging.  saviObjectsSystemNotifySpoofingNumber used for setting or obtaining the maximum number of log messages that can be output per interval.  saviObjectsSystemBindingCount used for obtaining the number of binding entries.  saviObjectsSystemFilteringCount used for obtaining the number of filtering entries.  Added the following object to SaviObjectsCountEntry:  saviObjectsCountFilterOctets used for obtaining the byte count for spoofed packets filtered by SAVI. |
| Modified | None | None | None |
| 5130EI-CMW710-R3506P08~5130EI-CMW710-R3111P02 | | | |
| New | None | None | None |
| Modified | None | None | None |
| 5130EI-CMW710-R3111P01 | | | |
| 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 |
| 5130EI-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 |
| 5130EI-CMW710-R3109P16~5130EI-CMW710-R3109P03 | | | |
| New | None | None | None |
| Modified | None | None | None |
| 5130EI-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 |
| 5130EI-CMW710-R3108P03~5130EI-CMW710-R3106P01 | | | |
| New | None | None | None |
| Modified | None | None | None |
| 5130EI-CMW710-R3106 | | | |
| New | First release | First release | First release |
| Modified | First release | First release | First release |

# Operation changes

## Operation changes in R3507P10

None

## Operation changes in R3507P09

None

## Operation changes in R3507P02

None

## Operation changes in R3507

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

## Operation changes in R3506P11

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

## Operation changes in R3506P10

None

## Operation changes in R3506P08

None

## Operation changes in R3506P06

#### The following commands were added to the default configuration file:

password-control enable

#

local-user admin

service-type terminal

authorization-attribute user-role network-admin

#

user-interface aux 1

authentication-mode scheme

#

undo password-control aging enable

undo password-control composition enable

undo password-control history enable

undo password-control length enable

password-control login idle-time 0

password-control login-attempt 3 exceed unlock

password-control update-interval 0

## Operation changes in R3506P02

None

## Operation changes in R3506

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

## Operation changes in R3208P16

None

## Operation changes in R3208P15

* For the HPE 5130-24G-4SFP+ EI Switch JG932A and HPE 5130-24G-4SFP+ EI Brazil Switch JG975A, this version modified the start-to-work temperature for fans from 88°C to 98°C.
* For the HPE 5130-24G-2SFP+-2XGT EI Switch JG938A switches, this version modified the start-to-work temperature for fans from 83°C to 93°C.

## Operation changes in R3208P12

* Adjusted the priority of the BFD MAD detection packets to optimize the BFD MAD feature.

## Operation changes in R3208P10

None

## Operation changes in R3208P08

#### Changed the ACL issuing operation

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

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

## Operation changes in 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 R3208

None

## Operation changes in R3207

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

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

## Operation changes in R3115P08

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

## Operation changes in R3115P07

None

## Operation changes in R3115P06

None

## Operation changes in R3115P05

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 R3111P01

None

## Operation changes in R3110

None

## Operation changes in R3109P16

None

## Operation changes in R3109P14

None

## Operation changes in R3109P09

Changed the OpenFlow packet-in rate limit from 200 PPS to 1000 PPS.

## Operation changes in R3109P07

The priorities of ACL resources were modified to save ACL resources.

Added support for issuing commands to an SSH server.

* Before modification, an SSH user cannot issue commands to a switch acting as an SSH server through SSH parameters.
* After modification, an SSH user can issue commands in batches to an SSH server through SSH parameters.

## Operation changes in R3109P05

None

## Operation changes in R3109P04

None

## Operation changes in R3109P03

Added support for portal configuration in the Web interface

* Before modification, portal configuration is not supported in the Web interface.
* After modification, portal configuration is supported in the Web interface.

## Operation changes in R3109P01

None

## Operation changes in R3108P03

None

## Operation changes in R3108P01

None

## Operation changes in R3106P01

None

## Operation changes in R3106

First release.

# Restrictions and cautions

If the authorization VLAN does not exist, the access device first creates the VLAN and then assigns the user access interface as an untagged member to the VLAN. If the authorization VLAN already exists, the access device directly assigns the user access interface as an untagged member to the VLAN.

To deploy Web authentication on a trunk or hybrid port, make sure the port PVID, the authorization VLAN ID, and the user VLAN ID are the same.

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

When you downgrade a software package with the BootROM version 142 or a later version to a software package with the BootROM version earlier than 142, the BootROM version 122, 130, 132, or 134 is not downgraded together with the software package version.

When the HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch (JG940A) and HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch (JG941A) supply power to some telephones through PoE, you must use crossover cables.

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

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

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

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

# Open problems and workarounds

None

# List of resolved problems

## Resolved problems in R3507P10

#### 202303021705

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

## Resolved problems in R3507P09

#### 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:

Enable flow sampling and specify the number of packets out of which flow sampling samples a packet in Ethernet interface view.

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.

#### 202107191086

* Symptom: After some 802.1X users come online, no authorization VLAN or VSI is assigned to them.
* Condition: This symptom occurs if the following operations are performed:

Both 802.1X authentication and MAC authentication are enabled on interface.

ACLs are assigned to MAC authentication users.

Users come online and then go offline.

VLANs or VSIs are assigned to 802.1X users.

#### 202103311306

* Symptom: Failed to delete a permanent static route.
* Condition: This symptom occurs if the following operations are performed:

Configure a permanent static route and specify a preference lower than common static routes for the permanent static route.

Change the output interface address of the permanent static route and change the permanent static route settings multiple times. The permanent static route is recursed to a common route or to Null 0.

Delete the permanent static route.

## Resolved problems in R3507

#### 202105110200

* Symptom: CVE-2021-29219, 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:

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.

The two ports learn MAC addresses from each other.

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.

#### 202008240177

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

## Resolved problems in R3506P08

#### 202007271063

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

## Resolved problems in R3506P06

#### 202005271313

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

#### 202005291034

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

#### 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:

Configure both MAC authentication and 802.1X authentication on a port.

Issue the same ACL to users.

#### 202005111273

* Symptom: The combo ports on all IRF subordinate devices go down after a master/subordinate switchover.
* Condition: This symptom occurs if the master/subordinate switchover occurs after the original master device reboots or the entire IRF fabric reboots.

## Resolved problems in R3506P02

#### 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.

## Resolved problems in R3506

#### 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.

#### 201904100097

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

#### 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.

## Resolved problems in R3208P15

#### 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 large amount of traffic with varying quintuples is sent to the CPU through fast forwarding.

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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/43271e13-e971-4ac2-b12d-84922a8ce36b$tabTitle=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.

## Resolved problems in R3208P12

#### 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.

#### 201808090750

* Symptom: In QMC, ports on the device panel cannot be managed.
* Condition: This symptom occurs if QMC is used to manage the device.

#### 201808160104

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

#### 201809050679

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

#### 201807310087

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

#### 201806050164

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

#### 201808140119

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

#### 201808070167

* Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
* Condition: This symptom occurs if the following operations are performed:

An interface is configured with both MAC authentication and Web authentication.

A user fails to pass MAC authentication.

#### 201808060785

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

#### 201807210046

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

#### 201807120164

* Symptom: Some UDP packets with the destination port number 6784 are lost.
* Condition: This symptom occurs if the following operations are performed:

Configure BFD MAD on an IRF fabric.

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:

Configure the AAA authentication method as HWTACACS or RADIUS.

A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

#### 201806120588

* Symptom: The panel of the device is not completely displayed on the Web interface.
* Condition: This symptom occurs if you log in to the Web interface of a device that has combo interfaces, and enter the Dashboard > System Utilization > View Details page.

#### 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.

#### 201807160277

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

#### 201807040644

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

#### 201807040637

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

#### 201807040593

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

## Resolved problems in R3208P10

#### 201807190555

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

#### 201808020501

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

#### 201807310087

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

#### 201806050164

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

#### 201808140119

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

#### 201808070167

* Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
* Condition: This symptom occurs if the following operations are performed:

An interface is configured with both MAC authentication and Web authentication.

A user fails to pass MAC authentication.

#### 201808060785

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

#### 201807210046

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

#### 201807120164

* Symptom: Some UDP packets with the destination port number 6784 are lost.
* Condition: This symptom occurs if the following operations are performed:

Configure BFD MAD on an IRF fabric.

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:

Configure the AAA authentication method as HWTACACS or RADIUS.

A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

#### 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.

#### 201807160277

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

#### 201807040644

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

#### 201807040637

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

#### 201807040593

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

## Resolved problems in R3208P08

#### 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:

Two devices form an IRF fabric. The IRF fabric is connected to the core device through a multichassis aggregate link.

The access device connects to the IRF fabric through an aggregate interface, and the aggregate interface is assigned to a port isolation group.

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:

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.

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:

The device is configured with multiport ARP entries.

Outgoing interface consistency check for ARP entries and MAC address entries is enabled.

#### 201805250699

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

#### 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:

The network has a large number of short TCP connections.

The device keeps receiving and sending packets.

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:

When the copper port of the combo interface is active, enable EEE and auto power-down on the combo interface.

Activate the fiber port of the combo interface.

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:

Configure the interface as an ARP trusted interface by using the arp detection trust command.

Assign the interface to an aggregation group.

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.

#### 201802070015

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

#### 201801300024

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

#### 201803260509

* Symptom: The bpdu-drop any command configuration does not take effect.
* Condition: This symptom occurs if the following operations are performed:

On an IRF fabric, configure BFD MAD. Execute the bpdu-drop any command on the IRF physical interfaces.

In system view, execute the undo stp global enable/stp global enable or reboot command. The STP status of interfaces changes.

#### 201803160619

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

#### 201803200427

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

#### 201802010956

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

#### 201801300586

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

#### 201803230514

* Symptom: After a device configured with port security is rebooted, users fail to come online through MAC authentication.
* Condition: This symptom occurs if the following operations are performed:

Enable port security, and set the port security mode to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt on an interface.

Save the configuration, and delete the .mdb configuration file.

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.

#### 201712230037

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

#### 201801040748

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

#### 201801180968

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

#### 201711290635

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

#### 201712210545

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

#### 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.

#### 201711230489

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

#### 201711230366

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

#### 201711230694

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

#### 201712040081

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

#### 201711280600

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

Connect an IP phone to an interface.

Configure voice VLAN and port security on the interface.

Remove the settings from the interface and reconfigure them on the interface.

#### 201711280538

* Symptom: MAC address entries of MAC authentication users do not age out after the users go offline.
* Condition: This symptom might occur if the following conditions exist:
  + A Layer 2 switch configured with the spanning tree feature exists between the device and the authentication clients.
  + The device is enabled with MAC authentication.
  + The aging timer for dynamic MAC address entries is set to a value greater than 60 seconds by using the mac-address timer aging seconds command.

#### 201710300395

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

#### 201711110038

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

#### 201709250409

* Symptom: The mirroring and STP settings are partially lost.
* Condition: This symptom occurs if the following operations are performed:

Delete some SNMP settings.

Save the configuration by using the save force command and reboot the device.

#### 201708280341

* Symptom: MAC authentication fails after certain operations are performed.
* Condition: This symptom might occur if the following operations are performed:

Enable port security, and set the port security mode to userlogin-secure-or-mac on an interface.

Save the configuration and upgrade the software, or reboot the switch and use a .cfg file to restore the configuration.

#### 201708280275

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

#### 201708280259

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

#### 201708280255

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

#### 201710300047

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

#### 201708280230

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

#### 201710260388

* Symptom: The device does not support the ACL deployed by the 802.1X authentication server.
* Condition: This symptom occurs 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.

#### 201708310208

* Symptom: Web authentication entries exist, and users of other authentication types fail authentication or fail to get authorized when a large number of users exist.
* Condition: This symptom might occur if the following operations are performed when Web authentication is disabled:

Configure the web-auth free-ip command.

Reboot the device.

#### 201710310028

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

#### 201710260631

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

#### 201710270144

* Symptom: The device fails to automatically execute the save force command.
* Condition: This symptom might occur if the save force command is added to the autocfg configuration file.

#### 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.

#### 201709040292

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

#### 201710270540

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

#### 201710200099

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

#### 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 R3208

#### 201704280459

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

#### 201704280459

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

#### 201704270120

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

#### 201704270120

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

#### 201707200766

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

#### 2016707110001

* Symptom: A terminal connected to an interface enabled with EEE cannot ping the switch.
* Condition: This symptom might occur if the terminal connects to the switch through an interface enabled with EEE.

## Resolved problems in R3207

None

## 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:

Connect the switch to a Cisco IP phone installed with a key expansion module.

Enable PoE on the interface connected to the phone.

Set the maximum power for the PoE-enabled interface.

#### 201508120317

* Symptom: The switch uses a software version earlier than R3109P09, and PoE and LLDP are bled on an interface. When the interface flaps, the switch irregularly generates the CFGMAN\_CFGCHANGED message to report configuration changes.
* Condition: This symptom might occur if the following conditions exist:
  + The switch uses a software version earlier than R3109P09.
  + PoE and LLDP are enabled on an interface, and the interface flaps.

#### 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.

## Resolved problems in R3115P07

#### 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.

#### 201701040586

* Symptom: The display vlan brief command cannot display information about VLANs numbered the multiple of 41.
* Condition: This symptom might occur if the number of VLANs on the switch reaches the upper limit.

#### 201611220420

* Symptom: The console port of an IRF master might be inaccessible.
* Condition: This symptom might occur if the tty and comsh processes run on different CPU cores.

#### 201611110196

* Symptom: In certain conditions, the display stp brief command displays incorrect status information for a port.
* Condition: This symptom might occur if the following operations are performed:

Enable STP on the switch and its peer device.

Enable loop detection on the port connected to the peer device, and disable STP on the peer device.

Execute the display stp brief command for the port.

#### 201702060403

* Symptom: The 5130-24G-2SFP+-2XGT EI JG938A/5130-48G-2SFP+-2XGT EI JG939A/130-24G-PoE+-2SFP+-2XGT (370W) EI JG940A/5130-48G-PoE+-2SFP+-2XGT (370W) EI JG941A 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.

#### 201702090546/201701100036

* Symptom: After an IRF fabric is rebooted, some subordinate switches fail to respond, and the CLI of these switches is inaccessible. Output from the display device command shows that these switches are in Fault state.
* Condition: This symptom might occur if the following conditions exist:

The IRF fabric contains dual-chip switches.

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.

#### 201701060282

* Symptom: The device generates the log message "RESEND\_RADIUS:Failed to allocate PktID".
* Condition: This symptom occurs if a large number of users come online and go offline frequently when the primary RADIUS accounting server and secondary RADIUS accounting servers are unreachable.

## 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:

Delete the startup.mdb and ifindex.dat files on the IRF member switches.

Save the configuration and reboot the IRF fabric.

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:

Create tunnel interfaces.

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 PC is directly connected to the switch's management interface and is configured as an NTP client.

An NTP server sends the switch NTP packets with the leap flag set to 01.

#### 201612060351

* Symptom: The dynamic MAC count is always displayed as 0.
* Condition: This symptom might occur if the display openflow instance command is used to display detailed information of an OpenFlow instance.

#### 201612050429

* Symptom: Port isolation does not take effect. Traffic statistics exist on other aggregation group member ports.
* Condition: This symptom might occur if the following operations are performed:

Configure an aggregation group and configure port isolation on its member ports.

Shut down all member ports by using the shutdown command or unplugging network cables.

Restore the member ports to the up state.

Send traffic to an aggregation group member port.

#### 201611250474

* Symptom: The device adds two layers of VLAN tags to an untagged packet.
* Condition: This symptom might occur if the following conditions exist:

Switch A and Switch B are directly connected through trunk ports. The trunk ports permit a VLAN.

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.

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:

Enable port security on the port and configure the limit on the number of secure MAC addresses.

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 user logs in to the device by using SSH.

The user enters incorrect passwords for three times.

The user fails to log in and is added to the blacklist.

The debugging information of the server is viewed.

#### 201610150081

* Symptom: Some users pass the authentication, but the MAC addresses of these users are not learned.
* Condition: This symptom might occur if the following conditions exist:
  + Five devices form an IRF fabric, including four S5130-52S-EI switches and one S5130-28S-EI switch.
  + Import the user configuration and enable MAC authentication on all ports.
  + Use an auxiliary device to bring up all the devices and perform authentication. The authentication users on each device are the same. As a result, these users are frequently moved among different devices.
  + Send authentication traffic for a period of time. Then, stop authentication traffic on four devices, and leave authentication traffic on only one device.

#### 201610260405

* Symptom: A user fails to log in to the device.
* Condition: This symptom might occur if the following conditions exist:

The tcp syn-cookies enable command is executed.

The Telnet client is not directly connected to the device.

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.

#### 201610260040

* Symptom: The logbuffer cannot continue to record more logs.
* Condition: This symptom might occur if the following conditions exist:
  + The info-center syslog min-age command is not configured.
  + Adjust the system running time to be earlier than the system time.
  + The logbuffer is full.

#### 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.

#### 201610260451

* Symptom: A user cannot use the correct username and password to log in to the device through the management interface or console interface.
* Condition: This symptom might occur if the password-control enable command is used to enable password control on the device and a large number of users use incorrect usernames and passwords to log in to the device.

#### 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:

Access the device through the Web interface.

On the Network > LLDP > LLDP-TLV page, select an interface, select 802.1TLVs QCN and DCBX, and apply the settings.

## Resolved problems in R3115P05

#### 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:

Both MAC authentication and 802.1X authentication are performed for the users, and MAC authentication is successful.

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:

The number of OUI addresses reaches the upper limit on the IRF fabric.

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.

#### 201609220002

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

#### 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.

#### 201607040335

* Symptom: A user cannot join the critical VLAN of MAC authentication when certain conditions exist.
* Condition: This symptom might occur if the following conditions exist:

The user fails MAC authentication and is assigned to the guest VLAN.

The authentication server becomes unavailable.

The reset mac-authentication guest-vlan command is executed.

#### 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.

#### 201609060439

* Symptom: The operating status of BFD MAD for IRF is Faulty.
* Condition: This symptom occurs if BAD MAD is enabled for both the IRF fabric and the peer device and the IRF fabric receives BFD MAD packets from the peer device.

#### 201607010063

* Symptom: Prompt messages occur in wrong order when the device decompresses a software image. The message that prompts users whether to delete the .ipe file appears before the message that prompts users to verify the legitimacy of the software image.
* Condition: This symptom occurs if the software of a member device is upgraded at the CLI by using the boot-loader command.

#### 201609070269

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

#### 201608310495

* Symptom: The error message "Scanning is interrupted" occurs during ARP scanning.
* Condition: This symptom occurs if ARP scanning for secondary address ranges is configured after the device software is upgraded to R3109P03 or a later software version.

#### 201608250027

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

#### 201507220217

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

## Resolved problems in R3115P01

#### 201605050154

* First found-in version: 5130EI-CMW710-R3113P02
* 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.

#### 201605180172

* Symptom: The undo speed auto downgrade and speed auto downgrade commands are executed on all ports of the device, and the running configuration is saved. After a reboot, automatic negotiation for speed downgrading is not enabled on all ports.
* Condition: This symptom might occur if the following operations are performed:
* Execute the undo speed auto downgrade and speed auto downgrade commands on all ports.
* Save the running configuration and reboot the switch.

#### 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

#### 201605250614

* Symptom: The speed auto a b  or speed auto a b c command is configured for an interface. After a reboot, only the  speed auto b or speed auto c  setting takes effect.
* Condition: his symptom might occur if the following operations are performed:
* Configure the speed auto a b or speed auto a b c command on the interface.

Save the configuration.

Reboot the device and use the .cfg configuration file to restore the configuration.

#### 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:

Use three switches to build an IRF fabric in a daisy-chain topology.

Power on the master member.

Power on subordinate member 1 and then subordinate member 2.

Save the configuration after the IRF fabric is formed.

#### 201601090054

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

#### 201603100197

* Symptom: On an inactivity aging-enabled interface, sticky MAC addresses age out before the secure MAC aging timer set by using the port-security timer autolearn aging command expires.
* Condition: This symptom might occur if the following operations are performed on an interface:
  + Enable port security and inactivity aging.
  + Use the port-security timer autolearn aging command to set the secure MAC aging timer.

## Resolved problems in R3113P03

#### [201604091715](javascript:openTab('../DefectDetail/Default/7d8b35f9-ab82-4e48-b577-f89e8486f69b',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201604091715');)

* 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

#### 201602010060

* Symptom: After the configuration of an IRF fabric is restored by using .cfg files, RIP route filtering configuration is lost.
* Condition: This symptom might occur if the following operations are performed:

Enable RIP on an IRF fabric.

Configure the filter-policy import or filter-policy export command for an interface on a subordinate switch.

Restore the configuration of the IRF fabric by using .cfg files.

#### 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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/f45f005e-9826-4b10-8e4e-605e65bee6da$tabTitle=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](javascript:openTab('../DefectDetail/Default/ed51debf-4f1a-4db7-96b4-d364ec382107',%20'问题单: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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/306e2230-055d-48ba-8236-da81e01de7d7$tabTitle=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.

#### 201510150328

* Symptom: The undo ssl version { tls1.0 | tls1.1 } disable command configuration does not take effect.
* Condition: This symptom occurs if the switch is operating in FIPS mode or non-FIPS mode.

#### 2[01512290192](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/7daff18b-9fbd-48bc-a82e-82eb0f69bd57%24tabTitle=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.

#### 2[01512290192](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/7daff18b-9fbd-48bc-a82e-82eb0f69bd57%24tabTitle=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.

#### 2[01512290192](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/7daff18b-9fbd-48bc-a82e-82eb0f69bd57%24tabTitle=201512290192)

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

#### 2[01512290192](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/7daff18b-9fbd-48bc-a82e-82eb0f69bd57%24tabTitle=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

#### 201602040025

* Symptom: After the lldp notification med-topology-change enable command is executed on a PoE-capable switch, the LLDP process exits unexpectedly and the IP phones connected to the PIs of the switch cannot operate correctly.
* Condition: This symptom might occur if the command is executed on a PoE-capable switch and IP phones are connected to the PIs of the switch.

#### [201601110412](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/8776011d-6f54-4039-a206-0211824c69d5$tabTitle=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.

#### 201603100197

* Symptom: On an inactivity aging-enabled interface, sticky MAC addresses age out before the secure MAC aging timer set by using the port-security timer autolearn aging command expires.
* Condition: This symptom might occur if the following operations are performed on an interface:
  + Enable port security and inactivity aging.
  + Use the port-security timer autolearn aging command to set the secure MAC aging timer.

#### 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](javascript:openTab('../DefectDetail/Default/5a9dd521-93ec-46bb-9836-a1efea7d8eaf',%20'%E9%97%AE%E9%A2%98%E5%8D%95:201512130013');)

* 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.

#### 201601130674

* Symptom: After a user exits the console login page, the user cannot log in to the switch again through the console port.
* Condition: This symptom occurs if the restore factory-default command is executed to restore factory default configuration.

#### 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.

#### 201511180177

* Symptom: A port cannot exit the guest VLAN.
* Condition: This symptom occurs if the following conditions exist:
  + The switch is enabled with 802.1X.
  + The port joins the 802.1X guest VLAN.
  + The MAC address of the MAC-VLAN entry has been learned by another port.

#### [201511190408](javascript:void(null);)

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

#### [201511190408](javascript:void(null);)

* 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](javascript:void(null);)

* 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](javascript:void(null);)

* 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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/96114b94-c8a2-4471-8d9e-95d0a40406a3$tabTitle=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

#### 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.

## Resolved problems in R3111P01

#### 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.

#### 201505150471

* Symptom: A subordinate switch in an IRF fabric cannot discover neighbors because it cannot forward LLDP frames.
* Condition: This symptom occurs if the l2protocol lldp tunnel dot1q command is configured on an interface on the subordinate switch.

#### 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.

## Resolved problems in R3110

#### 201511190084

* Symptom: The switch treats an Apply-Actions instruction in an OpenFlow flow entry as a Write-Actions instruction.
* Condition: This symptom occurs if the controller deploys a flow entry with an Apply-Actions instruction.

#### 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.

#### 201508170320

* Symptom: The value of the entPhysicalVendorType node for a transceiver module cannot be obtained through a MIB tool.
* Condition: This symptom occurs if the following operations have been performed:
  + Use the combo enable fiber command on a combo interface to activate its fiber combo port.
  + Install the transceiver module into the fiber combo port.

#### 201511170067

* Symptom: OpenFlow flow entries fail to be deployed.
* Condition: This symptom occurs if the controller deploys flow entries without actions to a flow table other than the first flow table of the multiple flow tables.

## Resolved problems in R3109P16

#### [201507160220](javascript:void(null);)

* 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](javascript:void(null);)

* 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](javascript:void(null);)

* 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](javascript:void(null);)

* 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](javascript:void(null);)

* 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](javascript:void(null);)

* 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.

#### 201509100463

* Symptom: The OpenFlow process restarts when the switch is receiving flow entries from the controller.
* Condition: This symptom might occur if the switch is receiving flow entries from the controller.

#### 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.

#### 201508120317

* Symptom: The poe max power configuration is automatically generated for an interface after the connected IP phone sends an LLDP frame to request power.
* Condition: This symptom might occur if the connected IP phone sends an LLDP frame to request power from the interface.

#### 201509010156

Symptom: The following switch models support the power design daughter card:

* HP 5130-24G-PoE+-4SFP+ (370W) EI Switch JG936A.
* HP 5130-48G-PoE+-4SFP+ (370W) EI Switch JG937A.
* HP 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch JG977A.
* HP 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch JG978A.

Condition: None.

#### 201506180249

* Symptom: CVE-2015-3143
* Condition: 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
* Condition: 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.

## Resolved problems in R3109P07

#### 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.

#### 201505150245

* Symptom: The switch cannot correctly send ARP packets to the controller.
* Condition: This symptom might occur if a .mdb binary configuration file is used to restore OpenFlow configuration.

#### 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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/721055a3-cfd3-4b21-a60b-6d37032ba23d$tabTitle=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.

#### 201504210120

* Symptom: The PSE status setting of an IRF fabric is missing after a subordinate switch is rebooted.
* Condition: This symptom might occur if the following conditions exist:
  +  The IRF fabric contains multiple members.
  +  The poe enable pse command is configured on the IRF fabric.
  +  The subordinate switch is a PoE switch.

#### 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.

#### 201504150187

* Symptom: CVE-2015-1799
* Condition: Authentication doesn’t protect symmetric associations against DoS attacks.

#### 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 R3109P04

#### 201505240023

* Symptom: A PoE switch fails to supply power over PoE to all PDs after the switch is power cycled.
* Condition: This symptom might occur after the switch is power cycled.

#### 201510130155

* Symptom: The switch fails to obtain an IP address across VLANs.
* Condition: This symptom might occur if the following conditions exist:
  + A Layer 3 firewall is not deployed between the switch and the DHCP server.
  + DHCP relay is enabled on the Layer 3 firewall, and DHCP snooping is enabled on the switch.

## Resolved problems in R3109P03

#### 201503310150

* Symptom: A PC cannot obtain an IP address from the DHCP server.
* Condition: This symptom occurs if the following conditions exist:
  + DHCP snooping is enabled by using the dhcp snooping enable command on the switch.
  + The private VLAN feature is configured on the switch.
  + An interface in a primary VLAN is connected to the DHCP server.
  + An interface in an associated secondary VLAN is connected to the PC.

#### 201504080340

* Symptom: A RADIUS server fails to identify Access-Request packets from the switch, and users fail the authentication.
* Condition: This symptom occurs if Access-Request packets include invalid attribute values, for example, attribute values that end with \0.

## 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.

#### 201412180459

* Symptom: Traffic is not forwarded based on an OpenFlow group entry as expected.
* Condition: This symptom occurs if the following operations have been performed:
  + Configure a group entry.
  + Deploy a flow entry and configure the flow entry to use the group entry for forwarding.
  + Modify the output port of the group entry.

#### 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](http://idms.h3c.com/Login?tabUrl=DefectDetail/Default/3361f273-a17b-44b3-b45e-ca202ccda4f9$tabTitle=201503020204)

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

#### 201412190083

* Symptom: The voice-vlan qos command does not take effect on an interface.
* Condition: This symptom occurs if CDP-compatible LLDP is configured to advertise voice VLAN information on the interface.

#### 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 R3108P03

#### 201412150184

* Symptom: The MAC address entry for a user successfully passing MAC authentication is aged before the offline detect timer expires.
* Condition: This symptom occurs when MAC authentication is enabled and the mac-authentication timer offline-detect command is used set the offline detect timer for MAC authentication.

#### 201501140409

* Symptom: A user passing MAC authentication must wait 60 seconds before triggering new MAC authentication.
* Condition: This symptom occurs when the following conditions exist:
  + MAC authentication is enabled on an interface.
  + A user that accesses the interface passes MAC authentication.
  + The shutdown and then undo shutdown commands are executed on the interface.

#### 201412150398

* Symptom: After the shutdown command is executed in an interface through which a user fails the 802.1X authentication, the interface is still in the 802.1X Auth-Fail VLAN configured for the interface.
* Condition: This symptom occurs when the following conditions exist:
  + The dot1x quiet-period command is used in system view to enable the quiet timer.
  + 802.1X is enabled on the interface.
  + An 802.1X Auth-Fail VLAN is configured on the interface.

#### 201412040514

* Symptom: The switch first replies with a barrier reply and then prompts an error.
* Condition: This symptom occurs when OpenFlow continues to deploy flow entries and sends barrier request messages after the deployed flow entries reach the specifications.

#### 201412310374

* Symptom: CVE-2014-9295.
* Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet.

#### 201410230226

* 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).

#### 201410230226

* 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.

#### 201501150467

* Symptom: PoE cannot supply power correctly.
* Condition: This symptom can be seen when the PoE chip becomes abnormal because of PoE communication errors.

#### 201501070257

* Symptom: The switch cannot communicate with a Cisco IP phone.
* Condition: This symptom can be seen when the following conditions exist:
  + The switch is directly connected to the Cisco IP phone.
  + CDP-compatible LLDP is enabled on the switch.
  + The sent LLDP protocol packets and CDP protocol packets carry voice VLAN TLVs.

#### 201407310086

* Symptom: The function of configuring the voice VLAN information that LLDP/CDP advertises does not take effect.
* Condition: This symptom can be seen when the lldp tlv-enable med-tlv network-policy *vlan-id* command is configured on an interface to specify the voice VLAN information that LLDP/CDP will advertise to IP phones.

## Resolved problems in R3108P01

#### 201410140175

* Symptom: The system displays configuration errors though the configuration has been issued to an interface.
* Condition: This symptom can be seen when you log in to the switch through the Web interface and shut down an IRF physical interface.

#### 201410210187

* Symptom: When a user performs MAC authentication, the system does not transmit information about the MAC authentication-enabled interface to the authentication server. As a result, the user fails to pass the authentication.
* Condition: This symptom can be seen after you log in to the switch through the Web interface and enable MAC authentication on the interface.

#### 201410200402

* Symptom: The number of 802.1X online users collected in the Web interface is different from the actual number of 802.1X online users.
* Condition: This symptom can be seen when 2000 users pass 802.1X authentication and come online.

#### 201408290076

* Symptom: PoE cannot be successfully enabled on a port.
* Condition: This symptom can be seen when you log in to the switch through the Web interface and enable PoE on the port.

#### 201410200322

* Symptom: The maximum power of a PSE cannot be restored to the original value.
* Condition: This symptom can be seen when the following procedure is performed:
  + Log in to the switch through the Web interface.
  + Input an incorrect value for the maximum PSE power.
  + Click Cancel.

#### 201410100091

* Symptom: A black screen appears on the Web login page for the switch.
* Condition: This symptom can be seen when you log in to the switch through the Web interface and test the cable connections for Ethernet interfaces of the switch multiple times.

#### 201312030126

* Symptom: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.
* Condition: Addressed SSRT101324. A security bulletin for SSRT101324 should be published in January 2014. Please see the security bulletin for additional details.

#### 201410210004

* Symptom: Device will tear down TCP connection in established state when receives wrong TCP packet.
* Condition: Only for those TCP connections in established state. When they receive TCP SYN packet which is carrying a sequence number falling into the connection receiving window, a RST packet will be sent and the connection will be dropped immediately.

#### 201406190088

* Symptom: CVE-2014-0224.
* Condition: This symptom can be seen when Open SSL Server is used.

#### 201408220480

* Symptom: CVE-2014-3508
* Condition: A flaw in OBJ\_obj2txt may cause pretty printing functions such as X509\_name\_oneline, X509\_name\_print\_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

#### [201406270104](javascript:openTab('../DefectDetail/Default/8a3a13d9-50f9-4676-92d0-71fc163635a5',%20'问题单:201406270104');)

* Symptom: The MAC address entries of an STP edge port are deleted if the network topology changes.
* Condition: This symptom might occur if a port is configured as an STP edge port, and network topology changes occur.

## Resolved problems in R3106P01

None

## Resolved problems in R3106

First release

# Support and other resources

## Accessing Hewlett Packard Enterprise Support

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

[www.hpe.com/assistance](http://www.hpe.com/assistance)

* To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

Information to collect:

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

## Documents

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

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

### Related documents

The following documents provide related information:

* HPE 5130 EI Switch Series Installation Guide
* HPE PSR150-A & PSR150-D Power Supplies User Guide
* HPE 5130 EI Switch Series Configuration Guides-Release 32xx
* HPE 5130 EI Switch Series Command References-Release 32xx

### 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.

1. Feature list
   1. Hardware features

Refer to *HPE 5130 EI Switch Series Installation Guide*

* 1. Software features
     + - 1. Software features of the 5130 EI series

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Feature | HPE 5130-24G-4SFP+ EI Switch / HPE 5130-24G-2SFP+-2XGT EI Switch/ HPE 5130-24G-4SFP+ EI Brazil Switch | HPE 5130-48G-4SFP+ EI Switch / HPE 5130-48G-2SFP+-2XGT EI Switch/ HPE 5130-48G-4SFP+ EI Brazil Switch | HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch / HPE 5130-24G-PoE+-2SFP+-2XGT (370W) EI Switch/ HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch | HPE 5130-24G-SFP-4SFP+ EI Switch | HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch / HPE 5130-48G-PoE+-2SFP+-2XGT (370W) EI Switch/ HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch |
| Forwarding mode | Store-forward | | | | |
| IRF | * + - * Ring topology       * Daisy chain topology       * LACP MAD       * ARP MAD       * ND MAD       * BFD MAD       * 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)       * QinQ and selective QinQ | | | | |
| VLAN mapping | * + - * One-to-one VLAN mapping       * Many-to-one VLAN mapping       * Two-to-two VLAN mapping | | | | |
| ARP | * + - * 1K entries       * 512 static entries       * Gratuitous ARP       * Common proxy ARP and local proxy ARP       * ARP source suppression       * ARP black hole       * ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings)       * Multiport ARP | | | | |
| ND | * + - * 512 entries       * 256 static entries | | | | |
| VLAN virtual interface | 32 | | | | |
| DHCP | * + - * DHCP client       * DHCP snooping       * DHCP relay agent       * DHCP server       * DHCPv6 server       * DHCPv6 relay agent       * DHCPv6 snooping | | | | |
| UDP helper | * + - * UDP helper | | | | |
| DNS | * + - * Static DNS       * Dynamic DNS       * IPv4 and IPv6 DNS | | | | |
| IPv4 unicast route | * + - * 512 static routes       * RIP       * Routing policies       * Policy-based routing | | | | |
| IPv6 unicast route | * + - * 256 static routes       * RIPng       * Routing policies       * Policy-based routing | | | | |
| BFD | * + - * Static route       * MAD | | | | |
| Multicast | * + - * IGMP snooping       * MLD snooping       * IPv4 and IPv6 multicast VLAN       * IPv4 and IPv6 PIM 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       * 128 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       * HWTACACS       * SSH 2.0       * Port isolation       * 802.1X       * Port security       * MAC-address-based authentication       * IP Source Guard       * HTTPS       * PKI       * EAD | | | | |
| 802.1X | * + - * Up to 2,048 users       * Port-based and MAC address-based authentication       * 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 | * + - * Debugging information output       * Ping and Tracert       * NQA       * Track       * Remote maintenance through Telnet       * 802.1ag       * 802.3ah       * DLDP | | | | |

1. Fixed security vulnerabilities
   1. Fixed security vulnerabilities in R3507P09
      * 1. 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"

* + - 1. 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.

* + - 1. 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).

1. 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.

* 1. 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.

* 1. 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.

System startup process



* 1. 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 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, 5130EI-CMW710-BOOT-R3115P01.bin and 5130EI-CMW710-SYSTEM-R3115P01.bin.

* 1. Upgrading from the CLI

This section uses a two-member IRF fabric as an example to describe how to upgrade software from the CLI. If you have more than two subordinate switches, repeat the steps for the subordinate switch to upgrade their software. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch. For more information about setting up and configuring an IRF fabric, see the installation guide and IRF configuration guide for the HPE 5130 EI switch series.

* + 1. Preparing for the upgrade

Before you upgrade software, complete the following tasks:

Log in to the IRF fabric through Telnet or the console port. (Details not shown.)

Identify the number of IRF members, each member switch's role, and IRF member ID.

<Sysname> display irf

MemberID Role Priority CPU-Mac Description

\*+1 Master 5 0023-8927-afdc ---

2 Standby 1 0023-8927-af43 ---

--------------------------------------------------

\* indicates the device is the master.

+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 0023-8927-afdb

Auto upgrade : no

Mac persistent : 6 min

Domain ID : 0

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

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

# Identify the free flash space of the master switch.

<Sysname> dir

Directory of flash:

0 -rw- 41424 Aug 23 2013 02:23:44 startup.mdb

1 -rw- 3792 Aug 23 2013 02:23:44 startup.cfg

2 -rw- 53555200 Aug 23 2013 09:53:48 system.bin

3 drw- - Aug 23 2013 00:00:07 seclog

4 drw- - Aug 23 2013 00:00:07 diagfile

5 drw- - Aug 23 2013 00:00:07 logfile

6 -rw- 9959424 Aug 23 2013 09:53:48 boot.bin

7 -rw- 9012224 Aug 23 2013 09:53:48 backup.bin

524288 KB total (453416 KB free)

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

<Sysname> dir slot2#flash:/

Directory of slot2#flash:/

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

1 -rw- 3792 Jan 01 2011 02:23:44 startup.cfg

2 -rw- 93871104 Aug 23 2013 16:00:08 system.bin

3 drw- - Jan 01 2011 00:00:07 seclog

4 drw- - Jan 01 2011 00:00:07 diagfile

5 drw- - Jan 02 2011 00:00:07 logfile

6 -rw- 13611008 Aug 23 2013 15:59:00 boot.bin

7 -rw- 9012224 Nov 25 2011 09:53:48 backup.bin

524288 KB total (453416 KB free)

Compare the free flash space of each member switch with the size of the software file to load. If the space is sufficient, start the upgrade process. If not, go to the next step.

Delete unused files in the flash memory to free space:

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

# Delete unused files from the flash memory of the master switch.

<Sysname> delete /unreserved flash:/backup.bin

The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y

Deleting the file permanently will take a long time. Please wait...

Deleting file flash:/backup.bin...Done.

# Delete unused files from the flash memory of the subordinate switch.

<Sysname> delete /unreserved slot2#flash:/backup.bin

The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y

Deleting the file permanently will take a long time. Please wait...

Deleting file slot2#flash:/backup.bin...Done.

* + 1. Downloading software images to the master switch

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

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

* FTP download from a server
* FTP upload from a client
* TFTP download from a server
  + - 1. Prerequisites

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

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

* + - 1. FTP download from a server

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

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

Run an FTP server program on the server, configure an FTP username and password, specify the working directory and copy the file, for example, newest.ipe, to the directory.

Execute the ftp command in user view on the IRF fabric to access the FTP server.

<Sysname> ftp 10.10.110.1

Trying 10.10.110.1...

Press CTRL+C to abort

Connected to 10.10.110.1(10.10.110.1).

220 FTP service ready.

User (10.10.110.1:(none)):username

331 Password required for username.

Password:

230 User logged in.

Enable the binary transfer mode.

ftp> binary

200 Type set to I.

Execute the get command in FTP client view to download the file from the FTP server.

ftp> get newest.ipe

227 Entering Passive Mode (10,10,110,1,17,97).

125 BINARY mode data connection already open, transfer starting for /newest.ipe

226 Transfer complete.

32133120 bytes received in 35 seconds (896. 0 kbyte/s)

ftp> bye

221 Server closing.

* + - 1. FTP upload from a client

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

To FTP upload a file from a client:

On the IRF fabric:

Enable FTP server.

<Sysname> system-view

[Sysname] ftp server enable

Configure a local FTP user account:

# Create the user account.

[Sysname] local-user abc

# Set its password and specify the FTP service.

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

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

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

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

[Sysname-luser-manage-abc] quit

[Sysname] quit

On the PC:

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

c:\> ftp 1.1.1.1

Connected to 1.1.1.1.

220 FTP service ready.

User(1.1.1.1:(none)):abc

331 Password required for abc.

Password:

230 User logged in.

Enable the binary file transfer mode.

ftp> binary

200 TYPE is now 8-bit binary.

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

ftp> put newest.ipe

200 PORT command successful

150 Connecting to port 10002

226 File successfully transferred

ftp: 32133120 bytes sent in 64.58 secs (497.60 Kbytes/sec).

* + - 1. TFTP download from a server

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

Run a TFTP server program on the server, specify the working directory, and copy the file, for example, newest.ipe, to the directory.

On the IRF fabric, execute the tftp command in user view to download the file to the root directory of the flash memory on the master switch.

<Sysname> tftp 10.10.110.1 get newest.ipe

Press CTRL+C to abort.

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

100 30.6M 0 30.6M 0 0 143k 0 --:--:-- 0:03:38 --:--:-- 142k

* + 1. Upgrading the software images

To upgrade the software images:

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

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

Verifying image file..........Done.

Images in IPE:

boot.bin

system.bin

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

Add images to target slot.

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

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

The images that have passed all examinations will be used as the main startup so

ftware images at the next reboot on slot 1.

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

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

Verifying image file..........Done.

Images in IPE:

boot.bin

system.bin

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

Add images to target slot.

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

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

The images that have passed all examinations will be used as the main startup so

ftware images at the next reboot on slot 2.

Enable the software auto-update function.

<Sysname> system-view

[Sysname] irf auto-update enable

[Sysname] quit

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

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

<Sysname> save

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(\*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait.................

Saved the current configuration to mainboard device successfully.

Slot 2:

Save next configuration file successfully.

Reboot the IRF fabric to complete the upgrade.

<Sysname> reboot

Start to check configuration with next startup configuration file, please wait.

........DONE!

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

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

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

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

* 1. 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 | TIP:  Upgrading through the Ethernet port is faster than through the console port. |

* + 1. Prerequisites

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

* + - 1. Setting up the upgrade environment

Use a console cable to connect the console terminal (for example, a PC) to the console port on the switch.

Connect the Ethernet port on the switch to the file server.

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

Run a terminal emulator program on the console terminal and set the following terminal settings:

* + Bits per second—9,600
  + Data bits—8
  + Parity—None

Stop bits—1

* + Flow control—None
  + Emulation—VT100
    - 1. 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.
  + - 1. Verifying that sufficient storage space is available

|  |  |
| --- | --- |
| IMPORTANT | 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.

* + - * 1. 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.”

* + - 1. 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.

* + 1. Accessing the Boot menu

Starting......

Press Ctrl+D to access BASIC BOOT MENU

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \*

\* HPE 5130-48G-4SFP+ EI Switch BOOTROM, Version 112 \*

\* \*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Copyright (c) 2010-2015 Hewlett-Packard Development Company, L.P.

Creation Date : Apr 13 2015, 14:45:33

CPU Clock Speed : 1000MHz

Memory Size : 1024MB

Flash Size : 512MB

CPLD Version : 001

PCB Version : Ver.B

Mac Address : 443192f992f1

PEX mode is disabled.

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

Press one of the shortcut key combinations at prompt.

* + - * 1. Shortcut keys

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

* + 1. 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):

* + - * 1. Basic Boot ROM menu options

| Option | Task |
| --- | --- |
| 1. Update full BootRom | Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port. |
| 2. Update extended BootRom | Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port. |
| 3. Update basic BootRom | Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port. |
| 4. Boot extended BootRom | Access the extended Boot ROM segment.  For more information, see Accessing the extended Boot menu. |
| 0. Reboot | Reboot the switch. |
| Ctrl+U: Access BASIC ASSISTANT MENU | Press Ctrl + U to access the BASIC ASSISTANT menu (see Table 8). |

* + - * 1. 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. |

* + 1. 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 5130 EI Switch Series Configuration Guides*.

Password recovery capability is enabled.

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8):

* + - * 1. 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. |
| Ctrl+Y: Change Work Mode | Change Work Mode. |
| Ctrl+C: Display Copyright | Display the copyright statement. |

* + - * 1. 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. |

* + 1. 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
  + - 1. Using TFTP to upgrade software images through the Ethernet port

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):

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

* + - * 1. 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. |

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

Enter Y to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter N.

Loading.........................................................................

................................................................................

................................................................................

................................................................Done!

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. |

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

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8): 0

* + - 1. Using FTP to upgrade software images through the Ethernet port

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):

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 :\*\*\*

* + - * 1. 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. |

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

Enter Y to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter N.

Loading.........................................................................

................................................................................

................................................................................

................................................................Done!

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

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

Image file boot.bin is self-decompressing...

Free space: 534980608 bytes

Writing flash...................................................................

................................................................................

...................................................................Done!

Image file system.bin is self-decompressing...

Free space: 525981696 bytes

Writing flash...................................................................

................................................................................

................................................................................

................................................................................

................................................................................

................................................................................

.......................................................................Done!

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8):0

|  |  |
| --- | --- |
|  | NOTE:  The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.  If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid. |

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

* + - 1. 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.

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):

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

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

Download baudrate is 115200 bps

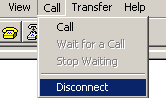
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

Press enter key when ready

Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.

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

Disconnecting the terminal from the switch



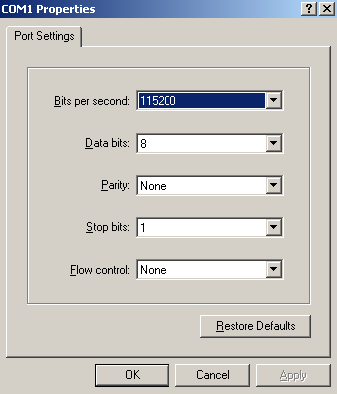
Select File > Properties, and in the Properties dialog box, click Configure.

Properties dialog box



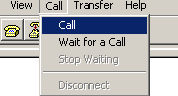
Select 115200 from the Bits per second list and click OK.

Modifying the baud rate



Select Call > Call to reestablish the connection.

Reestablishing the connection



Press Enter. The following prompt appears:

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

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

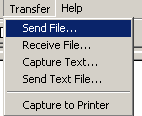
Now please start transfer file with XMODEM protocol

If you want to exit, Press <Ctrl+X>

Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC

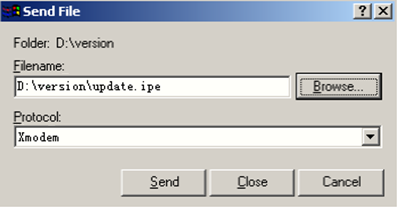
Select Transfer > Send File in the HyperTerminal window.

Transfer menu



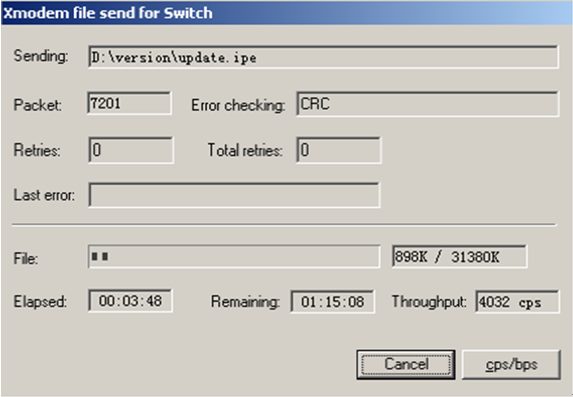
In the dialog box that appears, click Browse to select the source file, and select Xmodem from the Protocol list.

File transmission dialog box



Click Send. The following dialog box appears:

File transfer progress



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

Please input the file attribute (Main/Backup/None) m

The boot.bin image is self-decompressing...

# At the Load File name prompt, enter a name for the boot image to be saved to flash memory.

Load File name : default\_file boot-update.bin (At the prompt,

Free space: 470519808 bytes

Writing flash...................................................................

.............Done!

The system-update.bin image is self-decompressing...

# At the Load File name prompt, enter a name for the system image to be saved to flash memory.

Load File name : default\_file system-update.bin

Free space: 461522944 bytes

Writing flash...................................................................

.............Done!

Your baudrate should be set to 9600 bps again!

Press enter key when ready

|  |  |
| --- | --- |
|  | NOTE:  The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images 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. |

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

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

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8): 0

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

* + 1. 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
  + - 1. Using TFTP to upgrade Boot ROM through the Ethernet port

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):

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):

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

* + - * 1. 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. |

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

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

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

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

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

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

Updating extended BootRom? (Y/N):Y

Updating extended BootRom.........Done.

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):

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

* + - 1. Using FTP to upgrade Boot ROM through the Ethernet port

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):

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):

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

* + - * 1. 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. |

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

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

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

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

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

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

Updating extended BootRom? (Y/N):Y

Updating extended BootRom.........Done.

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):

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

* + - 1. 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.

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):

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):

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

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

Download baudrate is 115200 bps

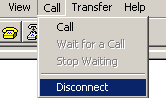
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

Press enter key when ready

Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.

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

Disconnecting the terminal from the switch



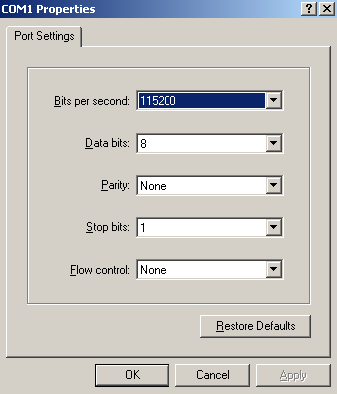
Select File > Properties, and in the Properties dialog box, click Configure.

Properties dialog box



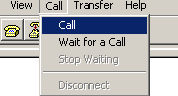
Select 115200 from the Bits per second list and click OK.

Modifying the baud rate



Select Call > Call to reestablish the connection.

Reestablishing the connection



Press Enter to start downloading the file.

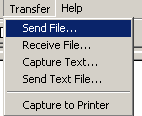
Now please start transfer file with XMODEM protocol

If you want to exit, Press <Ctrl+X>

Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC

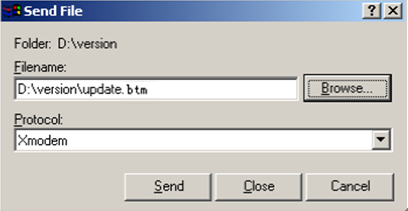
Select Transfer > Send File in the HyperTerminal window.

Transfer menu



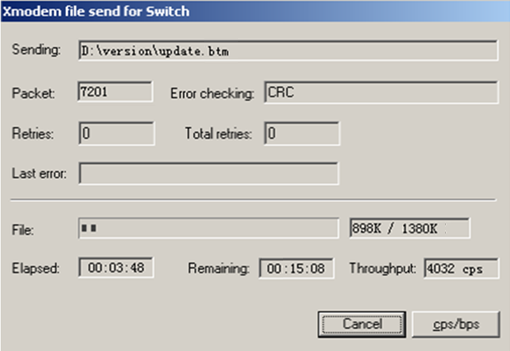
In the dialog box that appears, click Browse to select the source file, and select Xmodem from the Protocol list.

File transmission dialog box



Click Send. The following dialog box appears:

File transfer progress



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.

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

Updating extended BootRom? (Y/N):Y

Updating extended BootRom.........Done.

If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps at the prompt, as described in step 4.a. If the baud rate is 9600 bps, skip this step.

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

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

Press Enter to access the Boot ROM update menu.

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):

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

* + 1. 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.

* + - 1. Displaying all files

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

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8): 3

The following is a sample output:

Display all file(s) in flash:

File Number File Size(bytes) File Name

================================================================================

1 8177 flash:/testbackup.cfg

2(\*) 53555200 flash:/system.bin

3(\*) 9959424 flash:/boot.bin

4 3678 flash:/startup.cfg\_backup

5 30033 flash:/default.mdb

6 42424 flash:/startup.mdb

7 18 flash:/.pathfile

8 232311 flash:/logfile/logfile.log

9 5981 flash:/startup.cfg\_back

10(\*) 6098 flash:/startup.cfg

11 20 flash:/.snmpboots

Free space: 464298848 bytes

The current image is boot.bin

(\*)-with main attribute

(b)-with backup attribute

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

Deleting files

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

To delete files:

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

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

Enter Y at the confirmation prompt.

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

Deleting....................................Done!

* + - 1. 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:

Enter 2 in the Boot menu.

EXTENDED BOOT MENU

1. Download image to flash

2. Select image to boot

3. Display all files in flash

4. Delete file from flash

5. Restore to factory default configuration

6. Enter BootRom upgrade menu

7. Skip current system configuration

8. Set switch startup mode

0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU

Ctrl+F: Format file system

Ctrl+P: Change authentication for console login

Ctrl+R: Download image to SDRAM and run

Ctrl+Y: Change Work Mode

Ctrl+C: Display Copyright

Enter your choice(0-8): 2

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.

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

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

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!

* 1. Handling software upgrade failures

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

To handle a software upgrade failure:

Verify that the software release is compatible with the switch model and the correct file is used.

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.

Check the physical ports for a loose or incorrect connection.

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.

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.

Check the FTP or TFTP server for any incorrect setting.

Check that the storage device has sufficient space for the upgrade file.