Hewlett Packard Enterprise

HPE 5130EI-CMW710-R3115 Release Notes

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 5130EI-CMW710-R3115. Before you use this version in 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-R3115 Release Notes (Software Feature Changes)* and the documents listed in "Related documents"

Version information

Version number

HPE Comware Software, Version 7.1.045, Release 3115

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

Version history

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
5130EI-CMW710-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 Fixes bugs
5130EI-CMW710-R3113P05	R3113P03	2016-06-15	Release version	New features • PD detection mode Fixes bugs
5130EI-CMW710-R3113P03	R3113P02	2016-05-27	Release version	Fixes bugs
5130EI-CMW710-R3113P02	R3112	2016-05-06	Release version	New features • Automatic negotiation for speed downgrading • RADIUS stop-accounting packet buffering • HWTACACS stop-accounting packet

Version number	Last version	Release Date	Release type	Remarks
				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 Fixes bugs
5130EI-CMW710-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 • Fixes bugs
5130EI-CMW710-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 • Fixes bugs
5130EI-CMW710-R3111P03	R3111P02	2015-12-31	Release version	• New feature ○ Web authentication ○ Allowing link aggregation member ports to be in the deployed flow tables

Version number	Last version	Release Date	Release type	Remarks
				○ Transceiver module alarm suppression • Modified feature ○ 802.1X guest VLAN assignment delay • Fixes bugs
5130EI-CMW710-R3111P02	R3111P01	2015-12-28	Release version	• Fixes bugs
5130EI-CMW710-R3111P01	R3110	2015-12-18	Release version	• Fixes bugs
5130EI-CMW710-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 • Fixes bugs
5130EI-CMW710-R3109P16	R3109P14	2015-11-17	Release version	• New features: ○ Packet Capture • Fixes bugs
5130EI-CMW710-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

Version number	Last version	Release Date	Release type	Remarks
				○ 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 • Fixes bugs • HPE rebranding
5130EI-CMW710-R3109P09	R3109P07	2015-9-14	Release version	• New features: ○ L2PT • Fixes bugs

Version number	Last version	Release Date	Release type	Remarks
5130EI-CMW710-R3109P07	R3109P05	2015-7-31	Release version	• New features: ○ MAC authentication offline detection • Fixes bugs
5130EI-CMW710-R3109P05	R3109P04	2015-6-16	Release version	• Fixes bugs
5130EI-CMW710-R3109P04	R3109P03	2015-5-28	Release version	• Fixes bugs
5130EI-CMW710-R3109P03	R3109P01	2015-5-15	Release version	• New features: ○ RA Guard • Modified feature: Configuring the TCP maximum segment size (MSS) • Fixes bugs

5130EI-CMW710-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
				• Fixes bugs

5130EI-CMW710-R3108P03	R3108P01	2015-2-13	Release version	• New features:
				  ○ Disabling SSL 3.0
				  ○ Login delay
				  ○ ND Snooping
				• Fixes bugs

5130EI-CMW710-R3108P01	R3106	2014-12-12	Release version	Fixes bugs
5130EI-CMW710-R3106P01	R3106	2014-8-9	Release version	Add new hardware support
5130EI-CMW710-R3106	First release	2014-7-28	Release version	First release

Hardware and software compatibility matrix

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	5130 EI Series

Item	Specifications
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 145 or higher (Note: Use the **display version** command in any view to view the version information. Please see Note②)
Host software	5130EI-CMW710-R3115.ipe
iMC version	iMC BIMS 7.2 (E0402) iMC EAD 7.2(E0402) iMC TAM 7.2 (E0402) iMC UAM 7.2 (E0402) iMC NTA 7.2 (E0401) iMC PLAT 7.2 (E0403P04) iMC QoSM 7.2 (E0403) iMC RAM 7.2 (E0402) iMC SDNM 7.2 (E0402) iMC SHM 7.2 (E0402)
iNode version	iNode PC 7.2 (E0401)
Web version	None
Remarks	None

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

```
<HPE>display version
HPE Comware Software, Version 7.1.045, Release 3115            ------ Note①
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP
HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch uptime is 0 weeks, 0 days, 0 hours, 4 m
inutes
Last reboot reason : Cold reboot

Boot image: flash:/5130ei-cmw710-boot-r3115.bin
Boot image version: 7.1.045, Release 3115
  Compiled May 25 2016 16:00:00
System image: flash:/5130ei-cmw710-system-r3115.bin
System image version: 7.1.045, Release 3115
```

```
  Compiled May 25 2016 16:00:00


Slot 1:
Uptime is 0 weeks,0 days,0 hours,4 minutes
HPE 5130-48G-4SFP+ EI JG934A with 1 Processor
BOARD TYPE:         5130-48G-4SFP+ EI
DRAM:               1024M bytes
FLASH:              512M bytes
PCB 1 Version:      VER.B
Bootrom Version:    145                                          ------ Note②
CPLD 1 Version:     001
Release Version:    HPE 5130-48G-4SFP+ EI JG934A-3115
Patch Version  :    None
Reboot Cause   :    UserReboot
[SubSlot 0] 48GE+4SFP Plus
```

Upgrading restrictions and guidelines

None.

Hardware feature updates

5130EI-CMW710-R3115

None.

5130EI-CMW710-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

5130EI-CMW710-R3113P03

None.

5130EI-CMW710-R3113P02

None.

5130EI-CMW710-R3112

None.

5130EI-CMW710-R3111P07

None.

5130EI-CMW710-R3111P03

None.

5130EI-CMW710-R3111P02

None.

5130EI-CMW710-R3111P01

None.

5130EI-CMW710-R3110

None.

5130EI-CMW710-R3109P16

None.

5130EI-CMW710-R3109P14

None.

5130EI-CMW710-R3109P09

None.

5130EI-CMW710-R3109P07

None.

5130EI-CMW710-R3109P05

None.

5130EI-CMW710-R3109P04

None.

5130EI-CMW710-R3109P03

None.

5130EI-CMW710-R3109P01

None.

5130EI-CMW710-R3108P03

None.

5130EI-CMW710-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.

5130EI-CMW710-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.

5130EI-CMW710-R3106

First release.

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5130 EI-CMW710-R3115 Release Notes (Software Feature Changes)*.

MIB Updates

Table 3 MIB updates

Item	MIB file	Module	Description
5130EI-CMW710-R3115			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3113P05			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3113P03			
New	New	New	New
Modified	Modified	Modified	Modified
5130EI-CMW710-R3113P02			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3112			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3111P07			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
5130EI-CMW710-R3111P03			
New	None	None	None
Modified	None	None	None
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			
New	New	New	New
Modified	Modified	Modified	Modified
5130EI-CMW710-R3109P14			
New	New	New	New
Modified	Modified	Modified	Modified
5130EI-CMW710-R3109P09			
New	New	New	New
Modified	Modified	Modified	Modified

Item	MIB file	Module	Description
5130EI-CMW710-R3109P07			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3109P05			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3109P04			
New	None	None	None
Modified	None	None	None
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			
New	None	None	None
Modified	None	None	None
5130EI-CMW710-R3108P01			
New	None	None	None
Modified	None	None	None
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 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

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.

Open problems and workarounds

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.
- Workaround: Use the COA to issue an authorization ACL that carries the session-timeout attribute.

List of resolved problems

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:
  a. Configure the **speed auto a b** or **speed auto a b c** command on the interface.
  b. Save the configuration.
  c. 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:
  a. Use three switches to build an IRF fabric in a daisy-chain topology.
  b. Power on the master member.
  c. Power on subordinate member 1 and then subordinate member 2.
  d. Save the configuration after the IRF fabric is formed.

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

- 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:

  a. Enable RIP on an IRF fabric.

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

c. 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

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

201507300295

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

201604140100

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

201603120042

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

201603230420

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

201603230420

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

201603230420

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

201603230420

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

201603230420

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

201603230420

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

201603180535

- 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.

201603180535

- 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.

201512290192

- Symptom: CVE-2015-3194
- Condition: Fixed vulnerability which can be exploited in a DoS attack, if device is presented with a specific ASN.1 signature using the RSA.

201512290192

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

201512290192

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

201512290192

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

Resolved problems in R3112

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

- 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

- 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

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

201511190408

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

201511190408

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

201511190408

- Symptom: CVE-2015-7855

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

201501160412

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

201511230171

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

Resolved problems in R3111P02

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

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

201507160220

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

201507160220

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

201507160220

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

201507160220

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

201507160220

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

Resolved problems in R3109P14

201504130201

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

201509020039

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

201509160335

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

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

201506180249

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

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

- 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

- 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

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

  www.hpe.com/support/hpesc

Information to collect:

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

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

Documents

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

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

Related documents

The following documents provide related information:

- *HPE 5130 EI Switch Series Installation Guide*
- *HPE PSR150-A & PSR150-D Power Supplies User Guide*
- *HPE 5130 EI Switch Series Configuration Guides-Release 311x*
- *HPE 5130 EI Switch Series Command References-Release 311x*

Documentation feedback

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

Appendix A Feature list

Hardware features

Table 4 5130 EI series hardware features for non-PoE switch models

Item	HPE 5130-24G-4SFP+ EI	HPE 5130-48G-4SFP+ EI	HPE 5130-24G-SFP-4SFP+ EI
Dimensions (H × W × D)	43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in)	43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)
Weight	≤ 5 kg (11.02 lb)	≤ 5 kg (11.02 lb)	≤ 8 kg (17.64 lb)
Console ports	1	1	1
10/100/1000 Base-T Ethernet ports	24	48	8 (Each and its corresponding SFP port form a combo interface.)
100/1000Base-X SFP ports	N/A	N/A	24 (The rightmost eight SFP ports and their corresponding 10/100/1000Base-T Ethernet ports form combo interfaces.)
SFP+ ports	4	4	4
Power supply slots	N/A	N/A	2, on the rear panel

Input voltage	• Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz
	• Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
		• AC power source
		  ○ Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz
		  ○ Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
		• DC power source: –48 V DC power source in the equipment room or RPS (recommended HP RPS models: A-RPS800 or A-RPS1600)
		  ○ Rated voltage: –48 VDC to –60 VDC
		  ○ Max voltage: –36 VDC to –72 VDC	

Minimum power consumption	19 W	• AC: 38 W • DC: 38 W	• AC: 30 W • DC: 38 W
Maximum power consumption	26 W	• AC: 45 W • DC: 50 W	• AC: 60 W • DC: 68 W
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1		
Melting current of power supply fuse	AC-input: 2 A/250 V	• AC-input: 10 A/250 V • DC-input: 5 A/250 V	• AC-input: 5 A/250 V • DC-input: 8 A/250 V

Item	HPE 5130-24G-4SFP+ EI	HPE 5130-48G-4SFP+ EI	HPE 5130-24G-SFP-4SFP+ EI
Operating temperature	0°C to 45°C (32°F to 113°F)		
Operating humidity	5% to 95%, noncondensing		
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1		

Table 5 5130 EI series hardware features for PoE switch models

Item	HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch	HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch
Dimensions (H × W × D)	43.6 × 440 × 300 mm (1.72 × 17.32 × 11.81 in)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)
Weight	≤ 8 kg (17.64 lb)	≤ 8 kg (17.64 lb)
Console ports	1	1
10/100/1000Base-T Ethernet ports	24	48
SFP+ ports	4	4

Input voltage	• AC power source
	  ○ Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz
	  ○ Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
	• DC power source: HP A-RPS1600
	  ○ Rated voltage: –54 VDC to –57 VDC
	  ○ Max voltage: –44 VDC to –60 VDC for single DC input and –54 VDC to –57 VDC for AC+DC dual inputs	

Maximum PoE per port	30 W	30 W
Total PoE	AC: 370 W • DC: 740 W	• AC: 370 W • DC: 800 W
Minimum power consumption	AC: 30 W • DC: 25 W	• AC: 47 W • DC: 43 W
Maximum power consumption (including PoE consumption)	• AC: 460 W (including 370 W PoE consumption) • DC: 790 W (including 740 W PoE consumption)	• AC: 490 W (including 370 W PoE consumption) • DC: 890 W (including 800 W PoE consumption)
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	
Melting current of power supply fuse	• AC-input: 10 A/250 V • DC-input: 25 A/250 V	• AC-input: 10 A/250 V • DC-input: 25 A/250 V

Item	HPE 5130-24G-PoE+-4SFP+ (370W) EI Switch	HPE 5130-48G-PoE+-4SFP+ (370W) EI Switch
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	

Table 6 5130 EI series hardware features for more switch models

Item	HPE 5130-24G-2SFP+-2XGT EI Switch	HPE 5130-48G-2SFP+-2XGT EI Switch	HPE 5130-24G-PoE+-2SFP+-2XGT (370W) Switch	HPE 5130-48G-PoE+-2SFP+-2XGT (370W) Switch
Dimensions (H × W × D)	43.6 × 440 × 160 mm (1.72 × 17.32 ×6.3 in)	43.6 × 440 × 270 mm (1.72 × 17.32 × 9.55in)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)	43.6 × 440 × 420 mm (1.72 × 17.32 × 16.53 in)
Weight	≤ 3 kg (6.61 lb)	≤ 5 kg (11.02 lb)	≤ 6 kg (13.23 lb)	≤ 7 kg (15.43 lb)
Console ports	1	1	1	1
10/100/1000 Base-T Ethernet ports	24	24	48	48
SFP+ ports	2	2	2	2
Input voltage	• Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz • Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz	• AC power source ○ Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz ○ Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz • DC power source Rated voltage: S5130-28TP-EI：N/A S5130-52TP-EI: 36 VDC to –72 VDC S5130-28TP-PWR-EI: 54 VDC to –57 VDC S5130-52TP-PWR-EI: 54 VDC to –57 VDC		
Maximum PoE per port	N/A	N/A	30 W	30 W
Total PoE	N/A	N/A	• AC: 370 W • DC: 720 W	• AC: 370 W • DC: 800 W
Minimum power consumption	20 W	• AC: 36 W • DC: 36 W	• AC: 31 W • DC: 20 W	• AC: 43 W • DC: 30 W
Maximum power consumption	34 W	• AC: 54 W • DC: 54 W	• AC: 425 W (including 370 W PoE consumption) • DC: 750 W (including 720 W PoE consumption)	• AC: 470 W (including 370 W PoE consumption) • DC: 910 W (including 800 W PoE consumption)

Item	HPE 5130-24G-2SFP+ -2XGT EI Switch	HPE 5130-48G-2SFP +-2XGT EI Switch	HPE 5130-24G-PoE+ -2SFP+-2XGT (370W) Switch	HPE 5130-48G-PoE+ -2SFP+-2XGT (370W) Switch
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1			
Melting current of power module fuse	AC-input: 2 A/250 V	AC-input: 3.15 A/250 V	• AC-input: 10 A/250 V • DC-input: 25 A/250 V	• AC-input: 10 A/250 V • DC-input: 25 A/250 V
Operating temperature	0°C to 45°C (32°F to 113°F)			
Operating humidity	5% to 95%, noncondensing			
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1			

Table 7 5130 EI series hardware features for Brazil non-PoE switch models

Item	HPE 5130-24G-4SFP+ EI Brazil Switch	HPE 5130-48G-4SFP+ EI Brazil Switch
Dimensions (H × W × D)	43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in)	43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in)
Weight	≤ 5 kg (11.02 lb)	≤ 5 kg (11.02 lb)
Console ports	1	1
10/100/1000Base-T Ethernet ports	24	48
100/1000Base-X SFP ports	N/A	N/A
SFP+ ports	4	4
Power supply slots	N/A	N/A

Input voltage	• Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz
	• Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
		• AC power source
		  ○ Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz
		  ○ Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
		• DC power source: –48 V DC power source in the equipment room or RPS (recommended HP RPS models: A-RPS800 or A-RPS1600)
		  ○ Rated voltage: –48 VDC to –60 VDC
		  ○ Max voltage: –36 VDC to –72 VDC

Minimum power consumption	19 W	• AC: 38 W DC: 38 W

Item	HPE 5130-24G-4SFP+ EI Brazil Switch	HPE 5130-48G-4SFP+ EI Brazil Switch
Maximum power consumption	26 W	• AC: 45 W DC: 50 W
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	
Melting current of power supply fuse	AC-input: 2 A/250 V	• AC-input: 10 A/250 V • DC-input: 5 A/250 V
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	

Table 8 5130 EI series hardware features for Brazil PoE switch models

Item	HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch	HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch
Dimensions (H × W × D)	43.6 × 440 × 300 mm (1.72 × 17.32 × 11.81 in)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)
Weight	≤ 8 kg (17.64 lb)	≤ 8 kg (17.64 lb)
Console ports	1	1
10/100/1000Base-T Ethernet ports	24	48
SFP+ ports	4	4
Input voltage	• AC power source ○ Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz ○ Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz • DC power source: HP A-RPS1600 ○ Rated voltage: –54 VDC to –57 VDC ○ Max voltage: –44 VDC to –60 VDC for single DC input and –54 VDC to –57 VDC for AC+DC dual inputs	
Maximum PoE per port	30 W	30 W
Total PoE	AC: 370 W • DC: 740 W	• AC: 370 W • DC: 800 W
Minimum power consumption	AC: 30 W • DC: 25 W	• AC: 47 W • DC: 43 W
Maximum power consumption (including PoE consumption)	• AC: 460 W (including 370 W PoE consumption) • DC: 790 W (including 740 W PoE consumption)	• AC: 490 W (including 370 W PoE consumption) • DC: 890 W (including 800 W PoE consumption)

Item	HPE 5130-24G-PoE+-4SFP+ (370W) EI Brazil Switch	HPE 5130-48G-PoE+-4SFP+ (370W) EI Brazil Switch
Chassis leakage current compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	
Melting current of power supply fuse	• AC-input: 10 A/250 V • DC-input: 25 A/250 V	• AC-input: 10 A/250 V • DC-input: 25 A/250 V
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	• UL60950-1 • EN60950-1 • IEC60950-1 • GB4943.1	

Software features

Table 9 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
Full duplex Wire speed L2 switching capacity	128 Gbps	176 Gbps	128 Gbps	128 Gbps	176 Gbps
Whole system Wire speed L2 switching Packet forwarding rate	95.232 Mpps	130.952 Mpps	95.232 Mpps	95.232 Mpps	130.952 Mpps
Forwarding mode	Store-forward				

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
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				

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
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				

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
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)				

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
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				

Appendix B Upgrading software

This chapter describes types of software used on the switch and how to upgrade software while the switch is operating normally or when the switch cannot correctly start up.

System software file types

Software required for starting up the switch includes:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the switch cannot correctly start up.

- **Software images**—Includes boot images and system images.
  - **Boot image**—A .bin file that contains the operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
  - **System image**—A .bin file that contains the minimum modules required for device operation and some basic features, including device management, interface management, configuration management, and routing management.

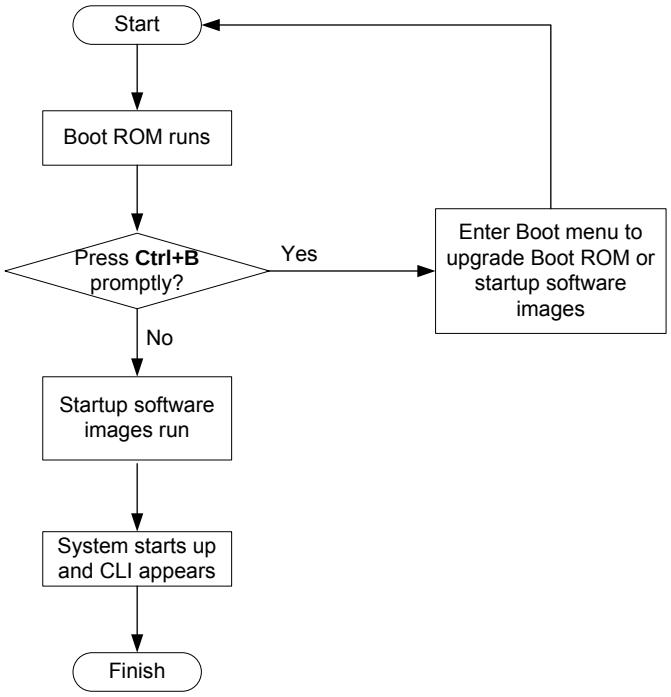
  The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

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

System startup process

Upon power-on, the Boot ROM image runs to initialize hardware and then the software images run to start up the entire system, as shown in Figure 1.

Figure 1 System startup process



Upgrade methods

You can upgrade system software by using one of the following methods:

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

The output in this document is for illustration only and might vary with software releases. This document uses boot.bin and system.bin to represent boot and system image names. The actual software image name format is *chassis-model_Comware-version_image-type_release*, for example, 5130EI-CMW710-BOOT-R3115.bin and 5130EI-CMW710-SYSTEM-R3115.bin.

Upgrading from the CLI

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

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

1. Log in to the IRF fabric through Telnet or the console port. (Details not shown.)
2. Identify the number of IRF members, each member switch's role, and IRF member ID.

```
<Sysname> display irf
MemberID   Role   Priority  CPU-Mac         Description
 *+1       Master  5         0023-8927-afdc  ---
   2       Standby 1         0023-8927-af43  ---
-------------------------------------------------
 * indicates the device is the master.
```

```
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 0023-8927-afdb
Auto upgrade               : no
Mac persistent             : 6 min
Domain ID                  : 0
```

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

IMPORTANT:

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

Identify the free flash space of the master switch.

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

524288 KB total (453416 KB free)
```

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

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:/
     0      -rw-       41424  Jan 01 2011 02:23:44     startup.mdb
     1      -rw-        3792  Jan 01 2011 02:23:44     startup.cfg
     2      -rw-    93871104  Aug 23 2013 16:00:08     system.bin
     3      drw-           -  Jan 01 2011 00:00:07     seclog
     4      drw-           -  Jan 01 2011 00:00:07     diagfile
     5      drw-           -  Jan 02 2011 00:00:07     logfile
     6      -rw-     13611008  Aug 23 2013 15:59:00     boot.bin
     7      -rw-     9012224  Nov 25 2011 09:53:48     backup.bin

524288 KB total (453416 KB free)
```

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

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

CAUTION:

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

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

```
<Sysname> delete /unreserved flash:/backup.bin
The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/backup.bin...Done.
# Delete unused files from the flash memory of the subordinate switch.
<Sysname> delete /unreserved slot2#flash:/backup.bin
The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file slot2#flash:/backup.bin...Done.
```

Downloading software images to the master switch

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

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

- FTP download from a server
- FTP upload from a client
- TFTP download from a server

Prerequisites

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

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

FTP download from a server

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

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

1. Run an FTP server program on the server, configure an FTP username and password, specify the working directory and copy the file, for example, **newest.ipe**, to the directory.
2. Execute the **ftp** command in user view on the IRF fabric to access the FTP server.

```
<Sysname> ftp 10.10.110.1
```

```
    Trying 10.10.110.1...
    Press CTRL+C to abort
Connected to 10.10.110.1(10.10.110.1).
    220 FTP service ready.
    User (10.10.110.1:(none)):username
    331 Password required for username.
    Password:
    230 User logged in.
```

3. Enable the binary transfer mode.

```
ftp> binary
  200 Type set to I.
```

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

```
ftp> get newest.ipe
  227 Entering Passive Mode (10,10,110,1,17,97).
  125 BINARY mode data connection already open, transfer starting for /newest.ipe
  226 Transfer complete.
  32133120 bytes received in 35 seconds (896. 0 kbyte/s)
ftp> bye
221 Server closing.
```

FTP upload from a client

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

To FTP upload a file from a client:

On the IRF fabric:

1. Enable FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

2. Configure a local FTP user account:

   # Create the user account.

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

   # Set its password and specify the FTP service.

```
[Sysname-luser-manage-abc] password simple pwd
[Sysname-luser-manage-abc] service-type ftp
```

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

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

On the PC:

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

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
```

```
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

4. Enable the binary file transfer mode.

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

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

```
ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 32133120 bytes sent in 64.58 secs (497.60 Kbytes/sec).
```

TFTP download from a server

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

1. Run a TFTP server program on the server, specify the working directory, and copy the file, for example, **newest.ipe**, to the directory.
2. On the IRF fabric, execute the **tftp** command in user view to download the file to the root directory of the flash memory on the master switch.

```
<Sysname> tftp 10.10.110.1 get newest.ipe
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 30.6M    0 30.6M    0     0   143k      0 --:--:--  0:03:38 --:--:--  142k
```

Upgrading the software images

To upgrade the software images:

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

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
Verifying image file.........Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin...................Done.
Decompressing file system.bin to flash:/system.bin...............Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 1.
```

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

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
Verifying image file.........Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin...................Done.
Decompressing file system.bin to flash:/system.bin...............Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 2.
```

3. Enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
[Sysname] quit
```

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

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

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.................
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
This command will reboot the device. Continue? [Y/N]:y
 Now rebooting, please wait...
```

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

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

NOTE:

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

Upgrading from the Boot menu

In this approach, you must access the Boot menu of each member switch to upgrade their software one by one. If you are upgrading software images for an IRF fabric, using the CLI is a better choice.

TIP:

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

Prerequisites

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

Setting up the upgrade environment

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

   NOTE:

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

3. Run a terminal emulator program on the console terminal and set the following terminal settings:
   - **Bits per second**—9,600
   - **Data bits**—8
   - **Parity**—None
   - **Stop bits**—1
   - **Flow control**—None
   - **Emulation**—VT100

Preparing for the TFTP or FTP transfer

To use TFTP or FTP:

- Run a TFTP or FTP server program on the file server or the console terminal.
- Copy the upgrade file to the file server.

- Correctly set the working directory on the TFTP or FTP server.
- Make sure the file server and the switch can reach each other.

Verifying that sufficient storage space is available

IMPORTANT:

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

When you upgrade software, make sure each member switch has sufficient free storage space for the upgrade file, as shown in Table 10.

Table 10 Minimum free storage space requirements

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.
Boot ROM	Same size as the Boot ROM upgrade image file.

If no sufficient space is available, delete unused files as described in "Managing files from the Boot menu."

Scheduling the upgrade time

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

Accessing the Boot menu

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU

********************************************************************************
*                                                                              *
*               HPE 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.

Table 11 Shortcut keys

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

Accessing the basic Boot menu

If the extended Boot ROM segment has corrupted, you can repair or upgrade it from the basic Boot menu.

Press **Ctrl+D** within 1 seconds after the "Press Ctrl+D to access BASIC BOOT MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended Boot ROM segment.

```
********************************************************************************
*                                                                              *
*                          BASIC BOOTROM, Version 112                          *
*                                                                              *
********************************************************************************

   BASIC BOOT MENU

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

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

Table 12 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 13).

Table 13 BASIC ASSISTANT menu options

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

Accessing the extended Boot menu

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

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

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 14). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 5130 EI Switch Series Configuration Guides*.

```
Password recovery capability is enabled.

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
```

```
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

Table 14 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.

Option	Tasks
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 15.
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

Table 15 EXTENDED ASSISTANT menu options

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

Upgrading Comware images from the Boot menu

You can use the following methods to upgrade Comware images:

- Using TFTP to upgrade software images through the Ethernet port
- Using FTP to upgrade software images through the Ethernet port
- Using XMODEM to upgrade software through the console port

Using TFTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

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

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

Table 16 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).

Item	Description
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

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

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

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

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

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

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

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash...............................................................
.............................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash...............................................................
.............................................................................
.............................................................................
.............................................................................
.............................................................................
.............................................................................
.....................................................Done!
```

NOTE:

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

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

```
EXTENDED BOOT MENU
```

```
1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

Using FTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **2** to set the FTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
FTP User Name       :switch
FTP User Password   :***
```

Table 17 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.

Item	Description
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

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

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

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

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

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

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

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash.....................................................................
.....................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................Done!

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
```

```
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

NOTE:

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

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

Using XMODEM to upgrade software through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **3** to set the XMODEM download baud rate.

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

Enter your choice(0-5):5
```

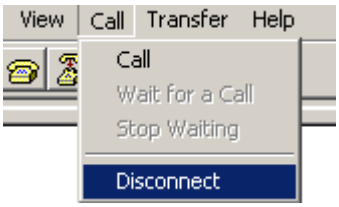
3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

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

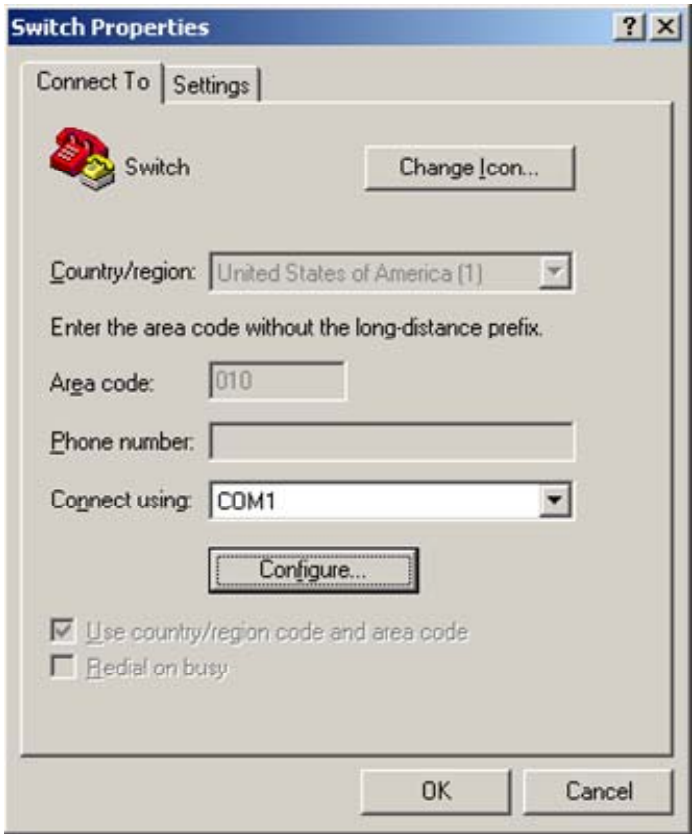
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



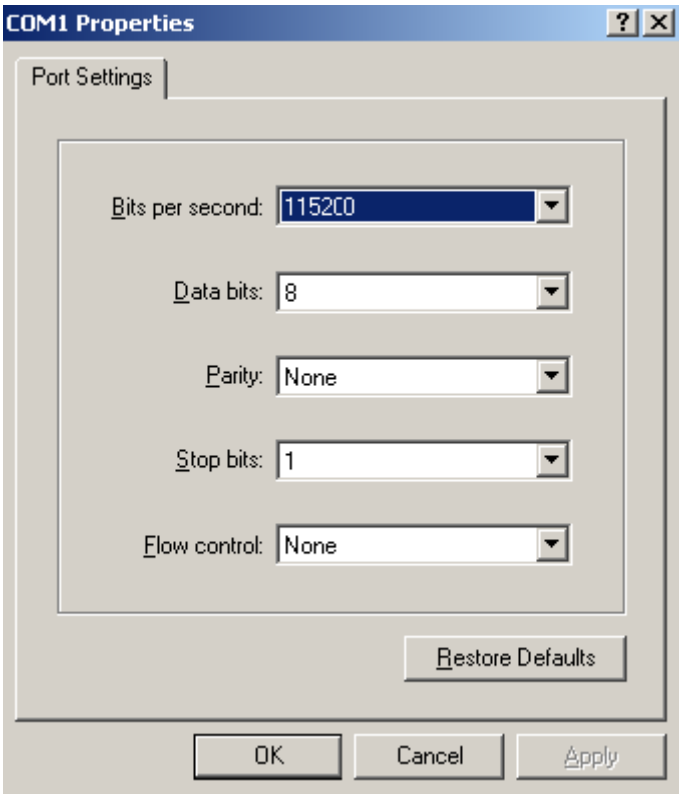
b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



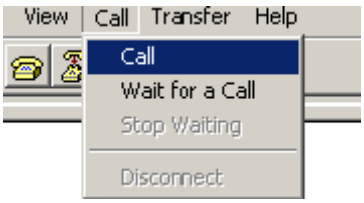
c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 4 Modifying the baud rate



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

Figure 5 Reestablishing the connection



5. Press **Enter**. The following prompt appears:

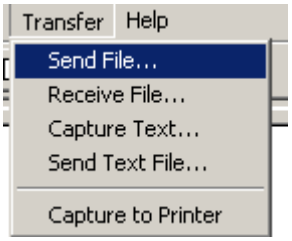
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

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

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

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

Figure 6 Transfer menu

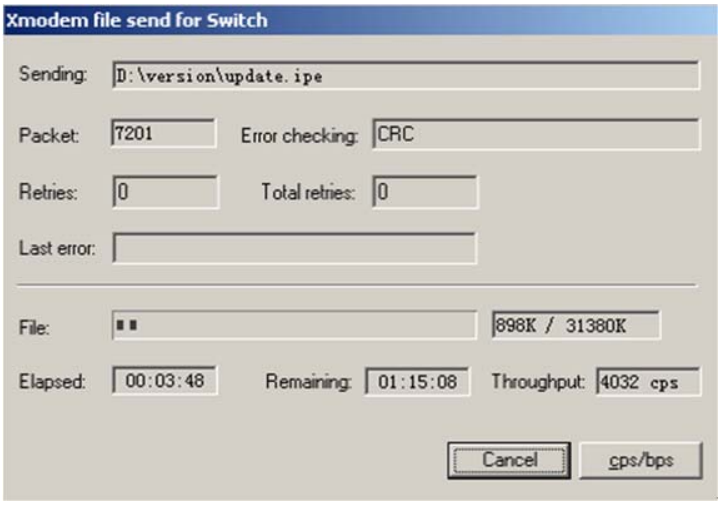


8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box

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

Figure 8 File transfer progress



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

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
```

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

```
Load File name  : default_file boot-update.bin       (At the prompt,
```

```
Free space: 470519808 bytes
Writing flash.....................................................................
.............Done!
The system-update.bin image is self-decompressing...
```

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

```
Load File name  : default_file system-update.bin
Free space: 461522944 bytes
Writing flash.....................................................................
.............Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

NOTE:

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

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

NOTE:

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

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

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

Upgrading Boot ROM from the Boot menu

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

- Using TFTP to upgrade Boot ROM through the Ethernet port
- Using FTP to upgrade Boot ROM through the Ethernet port
- Using XMODEM to upgrade Boot ROM through the console port

Using TFTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

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

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

Table 18 TFTP parameter description

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

NOTE:

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

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

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

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

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

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

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

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

Using FTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **2** to set the FTP parameters.

```
Load File Name     :update.btm
Server IP Address  :192.168.0.3
Local IP Address   :192.168.0.2
Subnet Mask        :255.255.255.0
Gateway IP Address :0.0.0.0
FTP User Name      :switch
FTP User Password  :123
```

Table 19 FTP parameter description

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

NOTE:

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

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

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

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

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

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

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

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

Using XMODEM to upgrade Boot ROM through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
```

```
Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **3** to set the XMODEM download baud rate.

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

Enter your choice(0-5):5
```

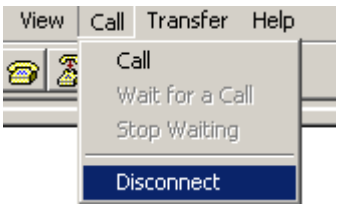
4. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

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

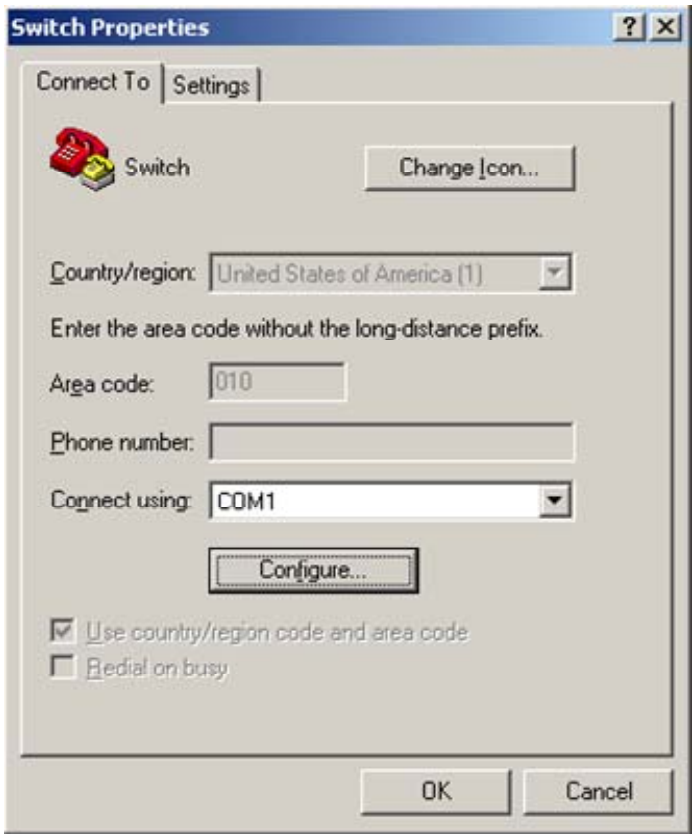
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



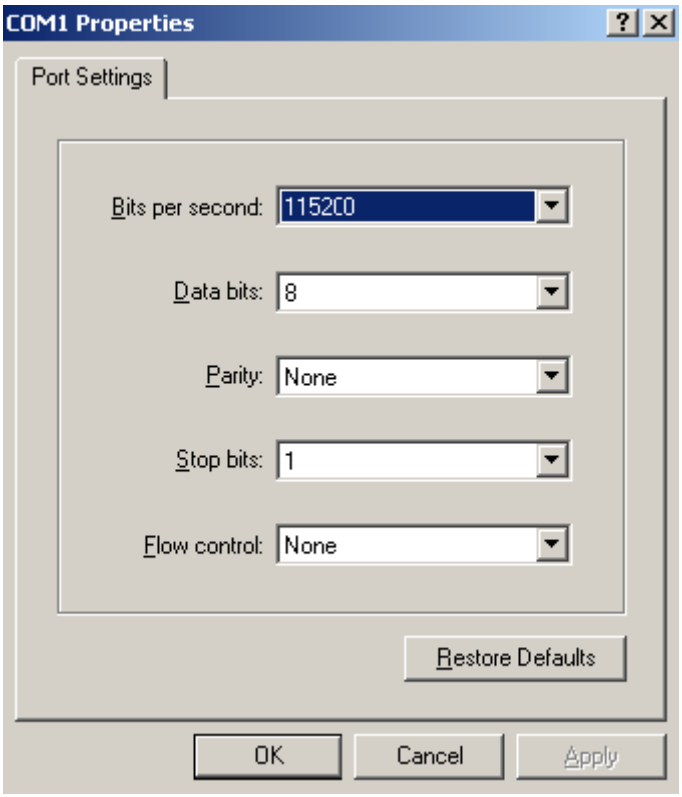
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



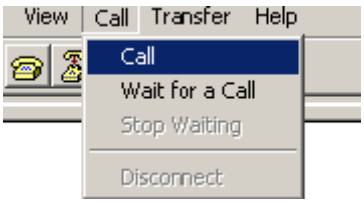
c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



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

Figure 12 Reestablishing the connection

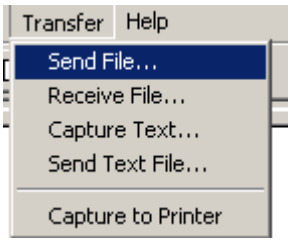


6. Press **Enter** to start downloading the file.

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

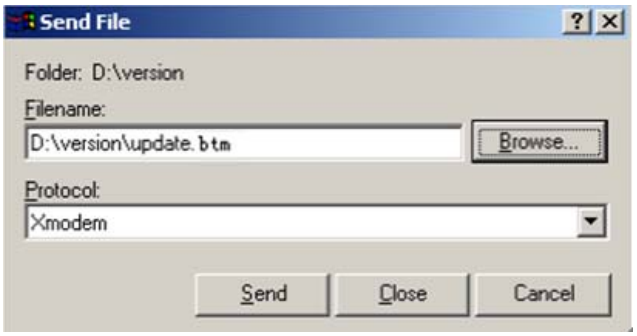
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



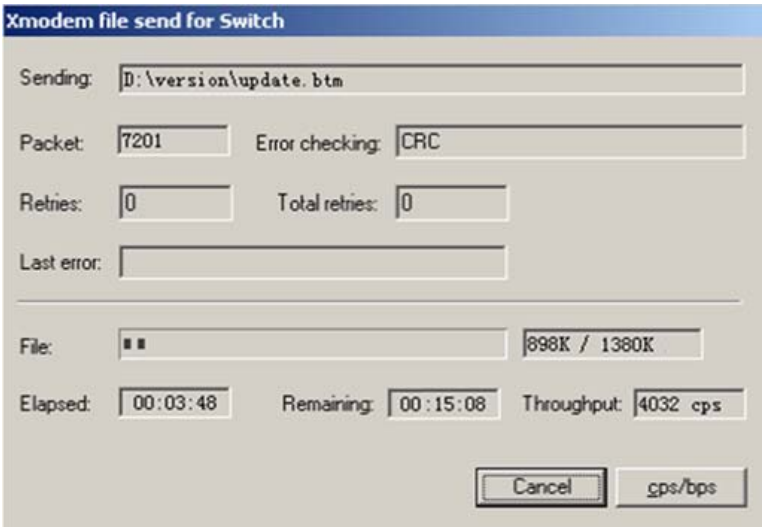
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 14 File transmission dialog box



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

Figure 15 File transfer progress



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

```
Loading ...CCCCCCCCCCCCC  ...Done!
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

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

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

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

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

NOTE:

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

13. Press **Enter** to access the Boot ROM update menu.
14. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

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

Managing files from the Boot menu

From the Boot menu, you can display files in flash memory to check for obsolete files, incorrect files, or space insufficiency, delete files to release storage space, or change the attributes of software images.

Displaying all files

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

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

    Enter your choice(0-8): 3
```

The following is a sample output:

```
Display all file(s) in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
```

```
4               3678                flash:/startup.cfg_backup
5               30033               flash:/default.mdb
6               42424               flash:/startup.mdb
7               18                  flash:/.pathfile
8               232311              flash:/logfile/logfile.log
9               5981                flash:/startup.cfg_back
10(*)           6098                flash:/startup.cfg
11              20                  flash:/.snmpboots
Free space: 464298848 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

Deleting files

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

To delete files:

1. Enter **4** in the Boot menu:

```
Deleting the file in flash:

File Number     File Size(bytes)     File Name
=============================================================================
1               8177                flash:/testbackup.cfg
2(*)            53555200            flash:/system.bin
3(*)            9959424             flash:/boot.bin
4               3678                flash:/startup.cfg_backup
5               30033               flash:/default.mdb
6               42424               flash:/startup.mdb
7               18                  flash:/.pathfile
8               232311              flash:/logfile/logfile.log
9               5981                flash:/startup.cfg_back
10(*)           6098                flash:/startup.cfg
11              20                  flash:/.snmpboots
Free space: 464298848 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

2. Enter the number of the file to delete. For example, enter **1** to select the file **testbackup.cfg**.

```
Please input the file number to change: 1
```

3. Enter **Y** at the confirmation prompt.

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

Changing the attribute of software images

Software image attributes include main (M), backup (B), and none (N). System software and boot software can each have multiple none-attribute images but only one main image and one backup

image on the switch. You can assign both the M and B attributes to one image. If the M or B attribute you are assigning has been assigned to another image, the assignment removes the attribute from that image. If the removed attribute is the sole attribute of the image, its attribute changes to N.

For example, the system image **system.bin** has the M attribute and the system image **system-update.bin** has the B attribute. After you assign the M attribute to **system-update.bin**, the attribute of **system-update.bin** changes to M+B and the attribute of **system.bin** changes to N.

To change the attribute of a system or boot image:

1. Enter **2** in the Boot menu.

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

Enter your choice(0-8): 2
```

2. **1** or **2** at the prompt to set the attribute of a software image. (The following output is based on the option **2**. To set the attribute of a configuration file, enter **3**.)

```
1. Set image file
2. Set bin file
3. Set configuration file
0. Return to boot menu

Enter your choice(0-3): 2

File Number    File Size(bytes)     File Name
============================================================================

1(*)              53555200              flash:/system.bin
2(*)              9959424               flash:/boot.bin
3                 13105152              flash:/boot-update.bin
4                 91273216              flash:/system-update.bin
Free space: 417177920 bytes
(*)-with main attribute
```

```
(b)-with backup attribute
(*b)-with both main and backup attribute
Note:Select .bin files. One but only one boot image and system image must be included.
```

3. Enter the number of the file you are working with. For example, enter 3 to select the boot image **boot-update.bin**. and enter **4** to select the system image **system-update.bin**.

```
Enter file No.(Allows multiple selection):3
Enter another file No.(0-Finish choice):4
```

4. Enter **0** to finish the selection.

```
Enter another file No.(0-Finish choice):0
You have selected:
flash:/boot-update.bin
flash:/system-update.bin
```

5. Enter **M** or **B** to change its attribute to main or backup. If you change its attribute to M, the attribute of **boot.bin** changes to none.

```
Please input the file attribute (Main/Backup) M
This operation may take several minutes. Please wait....
Next time, boot-update.bin will become default boot file!
Next time, system-update.bin will become default boot file!
Set the file attribute success!
```

Handling software upgrade failures

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

To handle a software upgrade failure:

1. Verify that the software release is compatible with the switch model and the correct file is used.
2. Verify that the software release and the Boot ROM release are compatible. For software and Boot ROM compatibility, see the hardware and software compatibility matrix in the correct release notes.
3. Check the physical ports for a loose or incorrect connection.
4. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
5. Check the file transfer settings:
   - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
   - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
   - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.
6. Check the FTP or TFTP server for any incorrect setting.
7. Check that the storage device has sufficient space for the upgrade file.