



Hewlett Packard
Enterprise

HPE 5120SI-CMW520-R1519P03

Release Notes

Contents

Version information	1
Version number	1
Version history	1
Hardware and software compatibility matrix	2
Upgrade restrictions and guidelines	4
Hardware feature updates	4
5120SI-CMW520-R1519P03	4
5120SI-CMW520-R1519P01	4
5120SI-CMW520-R1518P05	4
5120SI-CMW520-R1518P03	4
5120SI-CMW520-R1518P02	4
5120SI-CMW520-R1518P01	4
5120SI-CMW520-R1518	5
5120SI-CMW520-R1517P01	5
5120SI-CMW520-R1517	5
5120SI-CMW520-R1516P03	5
5120SI-CMW520-R1516P02	5
5120SI-CMW520-R1516	5
Software feature and command updates	5
MIB updates	5
Operation changes	6
Operation changes in R1519P03	6
Operation changes in R1519P01	7
Operation changes in R1518P05	7
Operation changes in R1518P03	7
Operation changes in R1518P02	7
Operation changes in R1518P01	7
Operation changes in R1518	7
Operation changes in R1517P01	7
Operation changes in R1517	7
Operation changes in R1516P03	7
Operation changes in R1516P02	7
Operation changes in R1516	7
Restrictions and cautions	8
Open problems and workarounds	8
List of resolved problems	9
Resolved problems in R1519P03	9
Resolved problems in R1519P01	11
Resolved problems in R1518P05	11
Resolved problems in R1518P03	12
Resolved problems in R1518P02	12
Resolved problems in R1518P01	13
Resolved problems in R1518	13
Resolved problems in R1517P01	13
Resolved problems in R1517	14
Resolved problems in R1516P03	14
Resolved problems in R1516P02	14
Resolved problems in R1516	14

Support and other resources	14
Accessing Hewlett Packard Enterprise Support	14
Documents	15
Related documents	15
Documentation feedback	15
Appendix A Feature list	16
Hardware features	16
Switch models	16
Technical specifications	16
Software features	18
Appendix B Upgrading software	22
Upgrading software from Boot ROM menus	22
Accessing the basic Boot menu	24
Accessing the extended Boot menu	25
Loading Software Using XMODEM through Console Port	27
Loading Software Using TFTP through Ethernet Port	34
Loading Software Using FTP through Ethernet Port	36
Upgrading at the CLI	38
Loading Software Using FTP	38
Loading Software Using TFTP	39

List of Tables

Version history.....	1
HPE 5120SI product family and HP A5120 family matrix	2
Hardware and software compatibility matrix	3
MIB updates	5
Table 1 Models in the HPE 5120 SI Switch Series	16
Table 2 HPE 5120 SI Switch Series technical specifications.....	16
Software features of the 5120 SI series.....	18
Table 3 Approaches to loading software on the switch	22
Table 4 Shortcut keys.....	23
Table 5 Basic Boot ROM menu options	24
Table 6 BASIC-ASSISTANT menu options	24
Table 7 Extended Boot ROM menu options.....	25
Table 8 EXTEND-ASSISTANT menu options	26
Table 9 Description of the TFTP parameters	35
Table 10 Description of the FTP parameters	37

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 5120SI-CMW520-R1519P03. 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 *5120SI-CMW520-R1519P03 Release Notes (Software Feature Changes)* and the documents listed in "[Related documents](#)"

Version information

Version number

Comware software, Version 5.20, Release 1519P03

Note: You can see the version number with the command **display version** in any view. See **Note ①**.

Version history

① IMPORTANT:

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

Version history

Version number	Last version	Release date	Release type	Remarks
5120SI-CMW520-R1519P03	5120SI-CMW520-R1519P01	2017-09-21	Release version	Fixes bugs.
5120SI-CMW520-R1519P01	5120SI-CMW520-R1518P05	2017-04-20	Release version	This version fixed bugs and introduced feature changes. New features include: <ul style="list-style-type: none"> Including user IP addresses in realtime accounting packets for MAC authentication users with dynamic IP addresses
5120SI-CMW520-R1518P05	5120SI-CMW520-R1518P03	2016-12-16	Release version	Fixes bugs.
5120SI-CMW520-R1518P03	5120SI-CMW520-R1518P02	2016-09-14	Release version	Fixes bugs.
5120SI-CMW520-R1518P02	5120SI-CMW520-R1518P01	2016-08-01	Release version	<ul style="list-style-type: none"> New feature: Support for NTP configuration in IPv6 Fixes bugs
5120SI-CMW520-R1518P01	5120SI-CMW520-R1518	2016-06-29	Release version	<ul style="list-style-type: none"> New feature: MAC authentication multi-VLAN mode on a port Fixes bugs

Version number	Last version	Release date	Release type	Remarks
5120SI-CMW520-R 1518	5120SI-CMW5 20-R1517P01	2016-06-02	Release version	Fixes bugs.
5120SI-CMW520-R 1517P01	5120SI-CMW5 20-R1517	2016-03-31	Release version	Fixes bugs.
5120SI-CMW520-R 1517	5120SI-CMW5 20-R1516P03	2016-03-02	Release version	Fixes bugs.
5120SI-CMW520-R 1516P03	5120SI-CMW5 20-R1516P02	2015-12-18	Release version	<ul style="list-style-type: none"> • New feature: Disabling alarm traps for transceiver modules • Fixes bugs
5120SI-CMW520-R 1516P02	5120SI-CMW5 20-R1516	2015-11-11	Release version	Fixes bugs.
5120SI-CMW520-R 1516	None	2015-10-22	Release version	First version

Hardware and software compatibility matrix

Before HPE 5120SI family, there were other product families, H3C S5120SI, shipped to market. All of these two product families have same hardware and software specification except brand. The product matrix is as following. In brief, the HPE 5120SI will be the representation to all of them in subsequent document.

HPE 5120SI product family and HP A5120 family matrix

HPE 5120SI and HP A5120 series	H3C S5120SI series
HPE 5120 8G PoE+ (65W) SI Switch	H3C S5120-9P-PWR-SI
HPE 5120 8G PoE+ (180W) SI Switch	H3C S5120-9P-HPWR-SI
HPE 5120 16G SI Switch	H3C S5120-20P-SI
HPE 5120 24G SI Switch	H3C S5120-28P-SI
HPE 5120 48G SI Switch	H3C S5120-52P-SI
HPE 5120 24G PoE+ (370W) SI Switch	H3C S5120-28P-HPWR-SI
HP A5120-16G SI Switch	H3C S5120-20P-SI
HP A5120-24G SI Switch	H3C S5120-28P-SI
HP A5120-48G SI Switch	H3C S5120-52P-SI
HP A5120-24G-PPoE+ SI Switch	H3C S5120-28P-PWR-SI
HP A5120-24G-PoE+ SI Switch	H3C S5120-28P-HPWR-SI

CAUTION:

To avoid an upgrade failure, use [Table 3](#) to verify the hardware and software compatibility before performing an upgrade.

Hardware and software compatibility matrix

Item	Specifications
Product family	5120 SI Switch Series
Hardware platform	HPE 5120 8G PoE+ (65W) SI Switch HPE 5120 8G PoE+ (180W) SI Switch HPE 5120 16G SI Switch HPE 5120 24G SI Switch HPE 5120 48G SI Switch HPE 5120 24G PoE+ (370W) SI Switch HP A5120-16G SI Switch HP A5120-24G SI Switch HP A5120-48G SI Switch HP A5120-24G-PPoE+ SI Switch HP A5120-24G-PoE+ SI Switch
Minimum memory requirements	128MB
Minimum Flash requirements	128 MB
Boot ROM version	Version 180 (Note: Use the display version command in any view to view the version information. See Note②)
System software image file	5120SI-CMW520-R1519P03.bin
iMC version	iMC BIMS 7.2 (E0402) iMC EAD 7.2 (E0402) iMC TAM 7.2 (E0402) iMC UAM 7.2 (E0402) iMC PLAT 7.2 (E0403P04) iMC QoSM 7.2 (E0403) iMC RAM 7.2 (E0402) iMC SHM 7.2 (E0402)
iNode version	iNode PC 7.2 (E0401)
Remarks	None

Display the system software version and Boot ROM version of the 5120 16G SI Switch:

```
<HPE>display version
HPE Comware Platform Software
Comware Software, Version 5.20, Release 1519P03 ----- Note①
Copyright (c) 2010-2017 Hewlett Packard Enterprise Development, L.P.
HPE 5120 16G SI Switch uptime is 0 week, 0 day, 0 hour, 19 minutes

HPE 5120 16G SI Switch
128M bytes DRAM
128M bytes Nand Flash Memory
Config Register points to Nand Flash

Hardware Version is REV.A
CPLD Version is 001
```

Bootrom Version is 180

----- Note②

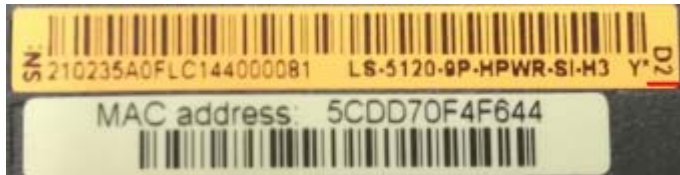
[SubSlot 0] 16GE+4SFP Hardware Version is REV.A

Upgrade restrictions and guidelines

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

The following switches must use R1517 or a later software version:

- The HPE 5120 8G PoE+ (180W) SI Switch with the code C0 that is vertically printed at the right end of the serial number label on the back panel.
- The HPE 5120 24G PoE+ (370W) SI Switch with the code E0 that is vertically printed at the right end of the serial number label on the back panel.



Hardware feature updates

5120SI-CMW520-R1519P03

None

5120SI-CMW520-R1519P01

None

5120SI-CMW520-R1518P05

None

5120SI-CMW520-R1518P03

None

5120SI-CMW520-R1518P02

None

5120SI-CMW520-R1518P01

None

5120SI-CMW520-R1518

The following flashes support 4-bit ECC:

- MICRON: MT29F1G08ABAEAWP:E
- SPANSION: S34ML01G200TFI003

5120SI-CMW520-R1517P01

None

5120SI-CMW520-R1517

None

5120SI-CMW520-R1516P03

None

5120SI-CMW520-R1516P02

None

5120SI-CMW520-R1516

None

Software feature and command updates

For more information about the software feature and command update history, see *5120SI-CMW520-R1519P03 Release Notes (Software Feature Changes)*.

MIB updates

MIB updates

Item	MIB file	Module	Description
5120-SI-CMW520-R1519P03			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1519P01			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
5120-SI-CMW520-R1518P05			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1518P03			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1518P02			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1518P01			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1518			
New	New	New	New
Modified	Modified	Modified	Modified
5120-SI-CMW520-R1517P01			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1517			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1516P03			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1516P02			
New	None	None	None
Modified	None	None	None
5120-SI-CMW520-R1516			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in R1519P03

None

Operation changes in R1519P01

None

Operation changes in R1518P05

None

Operation changes in R1518P03

None

Operation changes in R1518P02

None

Operation changes in R1518P01

None

Operation changes in R1518

None

Operation changes in R1517P01

None

Operation changes in R1517

None

Operation changes in R1516P03

None

Operation changes in R1516P02

None

Operation changes in R1516

None

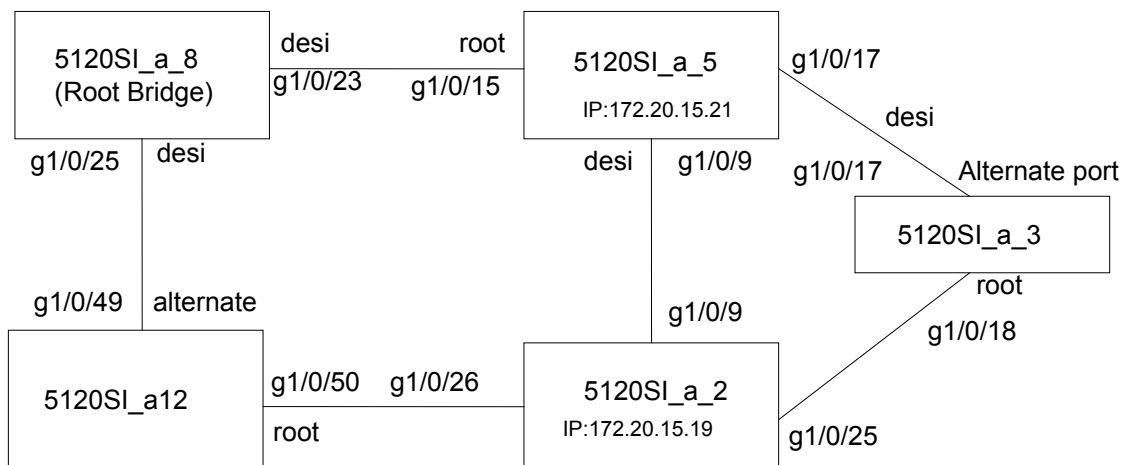
Restrictions and cautions

1. Do not power off the switch during a write operation, such as a save operation.
2. Displaying MAC addresses on a port does not show multicast MAC addresses.
3. Performing VCT check on an up port cannot detect the cable length.
4. The LED for a Gigabit SFP port blinks when the port is receiving packets, and is steady on when the port is sending packets.

Open problems and workarounds

LSD45818

- Symptom: As shown below, if RSTP/MSTP is disabled and then enabled on 5120SI_a_2, the g1/0/25 and g1/0/26 ports of 5120SI_a_2 cannot quickly change to the forwarding state.
- Condition: When RSTP/MSTP is enabled and then disables RSTP/MSTP on a device that resides in a similar position with 5120SI_a_2.



- Workaround: Do not perform such operations.

LSD68686

- Symptom: IMC fails to deploy a system software image to an IRF fabric that comprises two CPEs.
- Condition: When IMC is used to deploy a system software image to an IRF fabric comprising two CPEs. IMC can deploy a system software image to a single CPE.
- Workaround: None.

LSD070866

- Symptom: After the configuration file that contains the login password is saved and then the software is downgraded from the new version to a version earlier than F1509, a login attempt using the correct password fails.
- Condition: In this version of code, the password encryption within configuration files has been enhanced and cannot be interpreted by earlier revisions of the agent code. This means that if a unit is downgraded to earlier code, it may no longer be possible to login and manage the device.
- Workarounds:

- Before upgrading to the new code, it is necessary to ensure password control is disabled. Execute the “*undo password-control enable*” and then save this configuration file as a backup in case you need to downgrade the software again. If it is later necessary to downgrade to earlier software, force the switch to use this backup configuration file by executing a “*startup saved-configuration (filename)*” command before rebooting to the old code. Then, after the code has been downgraded, the device can be logged in from the console or by Telnet, but not SSH. The SSH authentication details will need to be reset.
- If no backup configuration has been saved but it is still possible to access the device management via some method while running the old code (e.g. Console, Telnet or SSH), then you can redefine all the device management passwords as required.
- If after a downgrade it is impossible to login to the device via any method, then there are two ways to recover the switch:
 - From the BOOT menu, set the new code to run again and reboot the device. Disable Telnet authentication:


```
User-interface vty 0 4
Authentication mode none
```

 Then save the configuration and downgrade the code again, login via Telnet and reset all the passwords as required.
 - From the BOOT menu. On boot-up, use Ctrl+B to enter the Boot menu and then force the unit to use the factory default configuration (bypassing the user configuration). The unit will then need to be fully reconfigured.

LSD071592

- Symptom: When a 1G port is connected to a device that uses the RTL8169 network chip of RealTek, the 1G port goes up and down twice, and then goes up.
- Condition: This symptom might occur when a 1G port is connected to a device that uses the RTL8169 network chip of RealTek.
- Workaround: None.

LSD074352

- Symptom: A PC fails to acquire an IPv6 address through DHCP.
- Condition: This symptom occurs if the switch port connected to the PC is configured with selective QinQ.
- Workaround: None.

List of resolved problems

Resolved problems in R1519P03

201704130233

- Symptom: After temperature alarm thresholds are restored to the default, the high-temperature alarming threshold is lower than the high-temperature warning threshold.
- Condition: This symptom might occur if temperature alarm thresholds are restored to the default.

201707240462

- Symptom: The system time is later than the UTC time if the switch has been running for a period of time.
- Condition: This symptom might occur if the switch has been running for a period of time.

201706230688

- Symptom: CVE-2012-2110
- Condition: Successfully exploiting this issue may allow an attacker to execute arbitrary code in the context of the application using the vulnerable library. Failed exploit attempts will result in a denial-of-service condition.

201708150501

- Symptom: The **undo packet-filter** command does not take effect on an interface.
- Condition: This symptom might occur if the **undo packet-filter** command is executed in interface view.

201706190117

- Symptom: The switch reboots unexpectedly when the ACL used by the **packet-filter** command is repeatedly configured, deleted, or displayed.
- Condition: This symptom might occur if the ACL used by the **packet-filter** command is repeatedly configured, deleted, or displayed.

201610090381

- Symptom: The switch reboots unexpectedly during configuration restoration if the number of ECMP routes exceeds the upper limit.
- Condition: This symptom might occur if the number of ECMP routes exceeds the upper limit.

201705040052

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

201707170477

- Symptom: Software upgrade fails if XMODEM is specified for software upgrade in the Boot menu.
- Condition: This symptom might occur if XMODEM is specified for software upgrade in the Boot menu.

201503110433

- Symptom: If a Telnet user repeatedly executes the **display interface** command, the following symptoms occur in sequence:
 - a. The CPU usage stays at 100 % for a period of time.
 - b. The memory is exhausted.
 - c. The PVST network topology changes.
- Condition: This symptom might occur if a Telnet user repeatedly executes the **display interface** command.

201704270120

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

201704270120

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

Resolved problems in R1519P01

201612050638

- Symptom: CVE-2016-7428
- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201612050638

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201612230172

- Symptom: CVE-2016-8610
- Condition: OpenSSL is prone to denial-of-service vulnerability. Successful exploitation of the issue will cause excessive memory or CPU resource consumption, resulting in a denial-of-service condition.

201703070076

- Symptom: When certain conditions exist, the subordinate switch in a dual-chassis IRF fabric cannot be accessed through the console port, and the display irf topology command does not display information about the subordinate switch.
- Condition: This symptom might occur if one of the following conditions exists:
 - The IRF fabric uses the ring topology, and it is rebooted.
 - The members of the IRF fabric are connected by two IRF links, and only one IRF link is up. When the IRF fabric is established, the down IRF link is brought up.

Resolved problems in R1518P05

201609010372

- Symptom: CVE-2013-0169
- Condition: The TLS protocol and the DTLS protocol do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

201609010389

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

201609010429

- Symptom: CVE-2014-9751
- Condition: The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly determine whether a source IP address is an IPv6 loopback

address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.

201609210337

- Symptom: CVE-2015-5219
- Condition: NTP is prone to a denial-of-service vulnerability. A remote attacker may exploit this issue to cause an infinite loop, resulting in a denial-of-service condition.

Resolved problems in R1518P03

201607210007

- Symptom: The device cannot be started, and reboots repeatedly.
- Condition: This symptom occurs if the device is rebooted after the **public-key peer** command is saved in the configuration file.

201607050188

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

201608230230

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

201608230230

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

201605170551

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

201605170551

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

Resolved problems in R1518P02

201601110113

- Symptom: A transient loop occurs on IRF physical interfaces.
- Condition: This symptom occurs after a cable is connected to and then disconnected from an

IRF physical interface.

201607260281

- Symptom: Time deviation exists between the device clock and the standard clock.
- Condition: This symptom occurs after the device is powered up and then runs for a period of time.

Resolved problems in R1518P01

201606080437

- Symptom: The output from the display this command does not contain the IPv4SG binding limit configured on an interface by using the ip verify source max-entries command.
- Condition: This symptom might occur if the ip verify source max-entries command is used to configure a limit for IPv4SG bindings on an interface.

201606020100

- Symptom: The switch drops a packet if its source MAC address belongs to an online MAC authentication user but the packet is not from the user's VLAN.
- Condition: This symptom might occur if the following conditions exist:
 - MAC authentication is enabled.
 - The source MAC address of a packet belongs to an online MAC authentication user, but the packet is not from the user's VLAN.

Resolved problems in R1518

201604260220

- Symptom: When an aggregate interface is disconnected, traffic is interrupted for 9 seconds rather than 6 seconds.
- Condition: This symptom occurs if the LACP timeout interval is set to the short timeout interval on an interface and the aggregate link is disconnected.

Resolved problems in R1517P01

201603150500

- Symptom: MFF accesses invalid memory and the switch reboots unexpectedly if certain conditions exist.
- Condition: This symptom might occur if the following conditions exist:
 - DHCP snooping and MFF are used together.
 - IP source guard generates IPSG bindings with invalid VLAN information based on DHCP snooping entries, and MFF uses these bindings.

201603150469

- Symptom: The switch keeps outputting the "System is busy with warm backup, please wait...." message.
- Condition: This symptom might occur if routing loops occur.

201603160244

- Symptom: The transfer distance and ordering name of an SFP-GE-LH70-SM1550 transceiver module are incorrect in the output from the display transceiver interface command.
- Condition: This symptom might occur if the display transceiver interface command is used to display information for an SFP-GE-LH70-SM1550 transceiver module.

Resolved problems in R1517

201512290219

- 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.

201412020201

- Symptom: An NMS retrieves only one MAC address entry when the NMS accesses the dot1dtpfdbtable MIB node.
- Condition: This symptom might occur if an NMS accesses the dot1dtpfdbtable MIB node.

Resolved problems in R1516P03

201510220051

- Symptom: VLAN authorization fails on an IRF fabric, and 802.1X users cannot pass authentication.
- Condition: This symptom might occur if 802.1X users come online when the IRF fabric is rebooting.

Resolved problems in R1516P02

201511100078

- Symptom: PoE cannot supply power.
- Condition: This symptom occurs when the switch uses a DC power supply and the input voltage is adjusted to 57V, approximately.

Resolved problems in R1516

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 FlexNetwork 5120 SI Switch Series Installation Guide
- HPE FlexNetwork 5120 SI Switch Series Configuration Guides-Release 1516
- HPE FlexNetwork 5120 SI Switch Series Command References-Release 1516

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

Switch models

Table 1 Models in the HPE 5120 SI Switch Series

Product code	HP description	Alias
JG310B	5120 8G PoE+ (65W) SI Switch	5120 8G-PoE+ (65W) SI
JG309B	5120 8G PoE+ (180W) SI Switch	5120 8G-PoE+ (180W) SI
JE073B	5120 16G SI Switch	5120 16G SI
JE074B	5120 24G SI Switch	5120 24G SI
JG091B	5120 24G PoE+ (370W) SI Switch	5120 24G PoE+ (370W) SI
JE072B	5120 48G SI Switch	5120 48G SI
JE073A	A5120-16G SI Switch	A5120-16G SI
JE074A	A5120-24G SI Switch	A5120-24G SI
JE072A	A5120-48G SI Switch	A5120-48G SI
JG092A	A5120-24G-PPoE+ SI Switch	A5120-24G-PPoE+ SI
JG091A	A5120-24G-PoE+ SI Switch	A5120-24G-PoE+ SI

Technical specifications

Table 2 HPE 5120 SI Switch Series technical specifications

Item	Description
Physical dimensions (H × W × D)	43.6 × 300 × 260 mm (1.72 × 11.81 × 10.24 in.) (5120 8G PoE+ (65W) SI) 43.6 × 300 × 260 mm (1.72 × 11.81 × 10.24 in.) (5120 8G PoE+ (180W) SI) 43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (5120 16G SI) 43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (5120 24G SI) 43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in.) (5120 48G SI) 43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in.) (5120 24G PoE+ (370W) SI) 43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (A5120-16G SI) 43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (A5120-24G SI) 43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in.) (A5120-48G SI) 43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in.) (A5120-24G-PPoE+ SI) 43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in.) (A5120-24G-PoE+ SI)
Weight	≤ 3 kg (6.61 lb) (5120-8G-PoE+ (65W) SI) ≤ 3 kg (6.01 lb) (5120-8G-PoE+ (180W) SI) ≤ 3 kg (6.61 lb) (5120-16G SI) ≤ 3 kg (6.61 lb) (5120-24G SI)

Item	Description
	<p>≤ 5 kg (11.02 lb) (5120-48G SI) ≤ 7 kg (15.43 lb) (5120-24G-PoE+ (370W) SI) ≤ 3 kg (6.61 lb) (A5120-16G SI) ≤ 3 kg (6.61 lb) (A5120-24G SI) ≤ 5 kg (11.02 lb) (A5120-48G SI) ≤ 6 kg (13.22 lb) (A5120-24G-PPoE+ SI) ≤ 7 kg (15.43 lb) (A5120-24G-PoE+ SI)</p>
Console port	1
Service ports	<p>8 × 10/100/1000Base-T autosensing Ethernet ports + 1 GE SFP interfaces (5120-8G-PoE+ (65W) SI) 8 × 10/100/1000Base-T autosensing Ethernet ports + 1 GE SFP interfaces (5120-8G-PoE+ (180W) SI) 16 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (5120-16G SI) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (5120-24G SI) 48 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (5120-48G SI) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (5120-24G-PoE+ (370W) SI) 16 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (A5120-16G SI) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (A5120-24G SI) 48 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (A5120-48G SI) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (A5120-24G-PPoE+ SI) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (A5120-24G-PoE+ SI)</p>
Input voltage	<p>AC: Rated voltage range: 100 VAC to 240 VAC, 50 Hz or 60 Hz Maximum voltage range: 90 VAC to 264 VAC, 47 Hz or 63 Hz DC: Use the external RPS unit provided by HPE only, with the rated voltage ranging from –52 VDC to –55 VDC Only 5120-24G-PoE+ (370W) SI and A5120-24G-PoE+ supports RPS DC input.</p>

Item	Description
Power consumption (full configuration)	25.1 W (5120-16G SI) 31.5 W (5120-24G SI) 59.8 W (5120-48G SI) 25.1 W (A5120-16G SI) 31.5 W (A5120-24G SI) 59.8 W (A5120-48G SI) 255 W (85 W for system power consumption and 170 W for PoE power consumption) (A5120-24G-PPoE+ SI) AC power input: 528 W (158 W for system power consumption and 370 W for PoE power consumption) (5120-24G-PoE+ (370W) and A5120-24G-PoE+ SI) DC power input: 832 W (92 W for system power consumption and 740 W for PoE power consumption) (5120-24G-PoE+ (370W) and A5120-24G-PoE+ SI) 95W (5120-8G-PoE+ (65W) SI) 230W (5120-8G-PoE+ (180W) SI)
Operating temperature	0°C to 45°C (32°F to 113°F)
Operating humidity (noncondensing)	10% to 90%

Software features

Software features of the 5120 SI series

Category	Features
Forwarding mode	Store and forward
IRF	An IRF fabric can comprise up to 4 devices.
Link aggregation	Dynamic aggregation of Gigabit Ethernet (GE) ports LACP Manual link aggregation Up to 26 link aggregation groups, each supporting up to eight GEs Load sharing
Flow control	IEEE 802.3x flow control and back pressure
Jumbo frame	Maximum frame size of 10 KB
MAC address table	8K MAC addresses 1K static MAC addresses Black hole MAC addresses MAC address learning limit on a port Static multicast MAC addresses
VLAN	Port-based VLANs (4094 VLANs) VLAN QinQ Protocol-based VLAN

Category	Features
	MAC-based VLAN GVRP ARP Snooping
ARP	256 entries 64 static entries ARP detection Gratuitous ARP
ND	8K entries 1K static entries ND detection
VLAN virtual interface	8
DHCP	DHCP client DHCP snooping DHCP relay agent DHCP server DHCPv6 client DHCPv6 snooping DHCPv6 server DHCPv6 relay agent
UDP helper	Supported
DNS	Static domain name resolution Dynamic domain name resolution client IPv4/IPv6 DNS
IP unicast route	IPv4/IPv6 static routes
Multicast	IGMP snooping MLD snooping Port-based multicast VLAN IPv6 multicast VLAN
Broadcast/multicast/unicast storm control	Storm control based on port rate percentage PPS-based storm control bps-based storm control
MSTP	STP/RSTP/MSTP/PVST protocol Up to sixteen spanning tree instances STP root protection BPDU protection
Smart Link	Smart link, up to 26 groups
Monitor link	Supported
QoS/ACL	802.1p/DSCP precedence marking L2 to L4 packet filtering Four queues per port SP, WRR, and SP+WRR queue scheduling algorithms Port-based line rate, with a minimum of 64-kbps granularity

Category	Features
	Flow-based traffic redirecting Time ranges VLAN ACL IPv6 ACL
Mirroring	Port mirroring Multi-monitor ports RSPAN remote mirroring
Security	Hierarchical management and password protection of users AAA authentication HWTACACS SSH 2.0 SSH v6 RADIUS authentication Port isolation 802.1X Port security MAC address authentication IP Source Guard HTTPS PKI SSL Password Control Portal EAD Triple authentication SAVI MAC authentication critical VLAN
802.1X	Up to 1024 users Port-based and MAC address-based authentication Guest VLAN Critical Vlan
Software download and upgrade	XModem FTP FTPV6 TFTP TFTPV6
Management	CLI configuration Remote configuration through Telnet Telnetv6 Console port SNMP SNMP v6 Remote Monitoring (RMON) alarm, event and history recording DM NMS

Category	Features
	Web NMS System log Log file Hierarchical alarms HGMPv2 NTP Power, fan, and temperature alarms PoE CWMP
Maintenance	Debugging information output Ping and Tracert Pingv6 and Tracertv6 NQA 802.3ah 802.1ag Remote maintenance through Telnet Virtual cable test DLDP Support RRPP

Appendix B Upgrading software

You can upgrade software from Boot ROM menus or the CLI.

Table 3 Approaches to loading software on the switch

Approach	Section
Upgrading from Boot ROM menus	Loading Software Using XMODEM through Console Port
	Loading Software Using TFTP through Ethernet Port
	Loading Software Using FTP through Ethernet Port
Upgrading from the CLI	Loading Software Using FTP
	Loading Software Using TFTP

Software images include the system software image and the Boot ROM image. They are packaged in a .bin file. You can download this file to upgrade both Boot ROM and system software, or upgrade only Boot ROM.

The Boot ROM image in the .bin package file consists of a basic segment and an extended segment. The basic segment is the minimum boot image. The extended segment enables the Boot ROM to bootstrap the system and upgrade system software.

! **IMPORTANT:**

When upgrading Boot ROM, upgrade both segments to ensure the functionality of the entire system.

Upgrading software from Boot ROM menus

The Boot ROM menus include a basic Boot menu and an extended Boot menu.

The basic Boot menu is provided by the basic Boot ROM segment. From this menu, you can upgrade Boot ROM and run the extended Boot ROM. For more information, see "[Accessing the basic Boot menu.](#)"

The extended Boot menu is provided by the extended Boot ROM segment. From this menu, you can perform various tasks, including upgrading Boot ROM, upgrading and managing system software images, and managing files. For more information, see "[Accessing the extended Boot menu.](#)"

Both the basic Boot menu and extended Boot menu support using XMODEM to upgrade Boot ROM through the console port.

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

NOTE:

The procedures for upgrading Boot ROM and system software from the extended Boot menu are the same except that you must choose different options from the Boot menu (1 for upgrading system software, and 6 for upgrading Boot ROM) to start the upgrade procedure. This appendix describes only the Boot ROM upgrade procedure.

To upgrade software from Boot ROM menus:

1. Connect a configuration terminal such as a PC to the console port of the switch with a console cable.
2. Run the terminal emulation program on the PC.

3. Power on the switch.

The switch starts up and displays the following message:

```
Starting.....
Press Ctrl+D to access BASIC BOOT MENU
Press Ctrl+T to start memory test

*****
*
*           HPE 5120 48G SI Switch BOOTROM, Version 177           *
*
*****
Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP.

Creation Date       : May  5 2015
CPU L1 Cache       : 32KB
CPU Clock Speed    : 333MHz
Memory Size        : 128MB
Flash Size         : 128MB
CPLD Version       : 002
PCB Version        : Ver.B
Mac Address        : 0000FE123456

Press Ctrl-B to enter Extended Boot menu...1
```

4. Press one of the shortcut key combinations at prompt.

Table 4 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 4 seconds after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.
Ctrl+T	Press Ctrl+T to start memory test	Performs a RAM self-test.	Press the keys within 4 seconds after the message appears. Alternatively, you can choose option 1 from the BASIC-ASSISTANT menu to perform the task.

Accessing the basic Boot menu

To access the basic Boot menu:

1. Press Ctrl+D within 4 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 177
*
*
*****
```

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 5 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 Loading Software Using XMODEM through 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 Loading Software Using XMODEM through 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 Loading Software Using XMODEM through 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 11).

Table 6 BASIC-ASSISTANT menu options

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

Option	Task
2. Reserved	Reserved option field.
3. Reserved	Reserved option field.
0. Return to boot menu	Return to the basic Boot menu.

Accessing the extended Boot menu

To access the extended Boot menu:

1. 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.

BootRom password: Not required. Please press Enter to continue.

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

2. Press **Enter** at the prompt for password.

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 12](#)). For more information about password recovery capability, see 5120SI-CMW520-R1516 Release Notes (Software Feature Changes).

Password recovery capability is enabled

BOOT MENU

1. Download application file to flash
 2. Select application file 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. Reserved
 9. Set switch startup mode
 0. Reboot
- Ctrl+F: Format File System
Ctrl+P: Skip Super Password
Ctrl+R: Download application to SDRAM and Run
Ctrl+Z: Access EXTEND-ASSISTANT MENU

Enter your choice(0-9):

Table 7 Extended Boot ROM menu options

Option	Tasks
1. Download application file to flash	<p>Download a .bin software package file to the flash.</p> <p>If password recovery capability is enabled, you can use any version of the system software image for upgrade.</p> <p>If password recovery capability is disabled, you can use only the Release 1516 version (or higher) for upgrade.</p>

Option	Tasks
2. Select application file to boot	Specify the main and backup system software images for the next startup: <ul style="list-style-type: none"> If password recovery capability is enabled, you can specify a system software image of any version. If password recovery capability is disabled, the system software image version must be R1516 or higher.
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. If password recovery capability is enabled, you can upgrade the Boot ROM to any version. If password recovery capability is disabled, you can upgrade the Boot ROM to only Version 160 or higher.
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. Reserved	Reserved option field.
9. 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: Skip Super Password	Load the next-startup configuration file with all user privilege passwords configured with the super password command ignored. 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 application to SDRAM and Run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTEND-ASSISTANT MENU	Access the EXTEND-ASSISTANT menu. For options in the menu, see Table 13 .

Table 8 EXTEND-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.

Loading Software Using XMODEM through Console Port

You can connect a PC or terminal to the console port to download files to the switch by using XMODEM. XMODEM supports 128-byte data packets and provides the reliability mechanisms including checksum, CRC, and retransmissions (up to 10).

Setting terminal parameters

Run a terminal emulator program on the console terminal, for example, a PC.

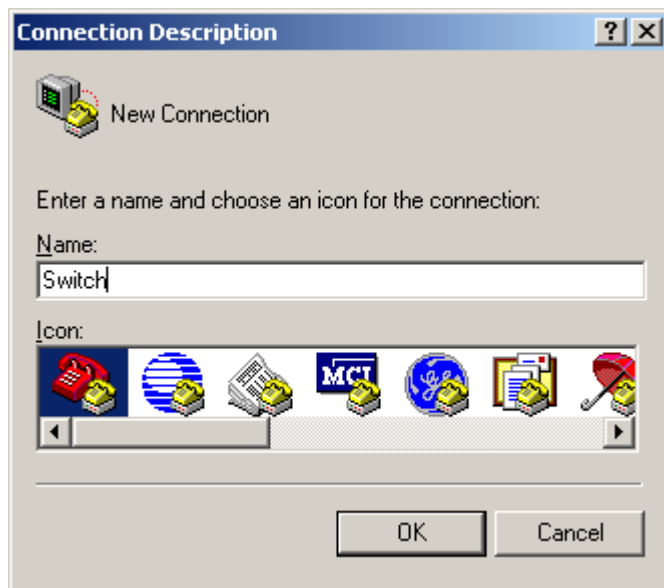
The following are the required terminal settings:

- Bits per second—9,600
- Data bits—8
- Parity—None
- Stop bits—1
- Flow control—None
- Emulation—VT100

Follow these steps to set terminal parameters, for example, on a Windows XP HyperTerminal:

1. Select **Start > All Programs > Accessories > Communications > HyperTerminal**, and in the **Connection Description** dialog box that appears, type the name of the new connection in the **Name** text box and click **OK**.

Figure 1 Connection description of the HyperTerminal



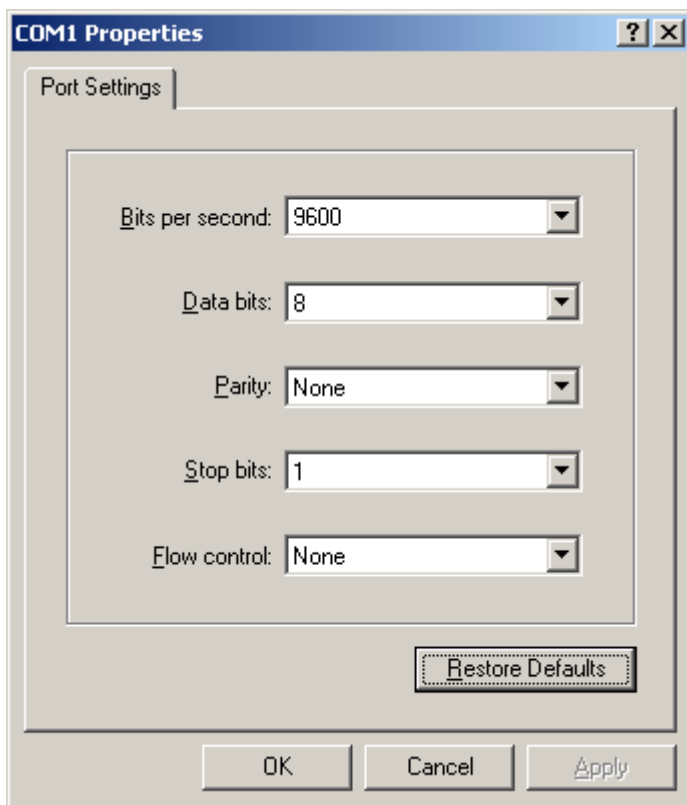
2. Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

Figure 2 Set the serial port used by the HyperTerminal connection



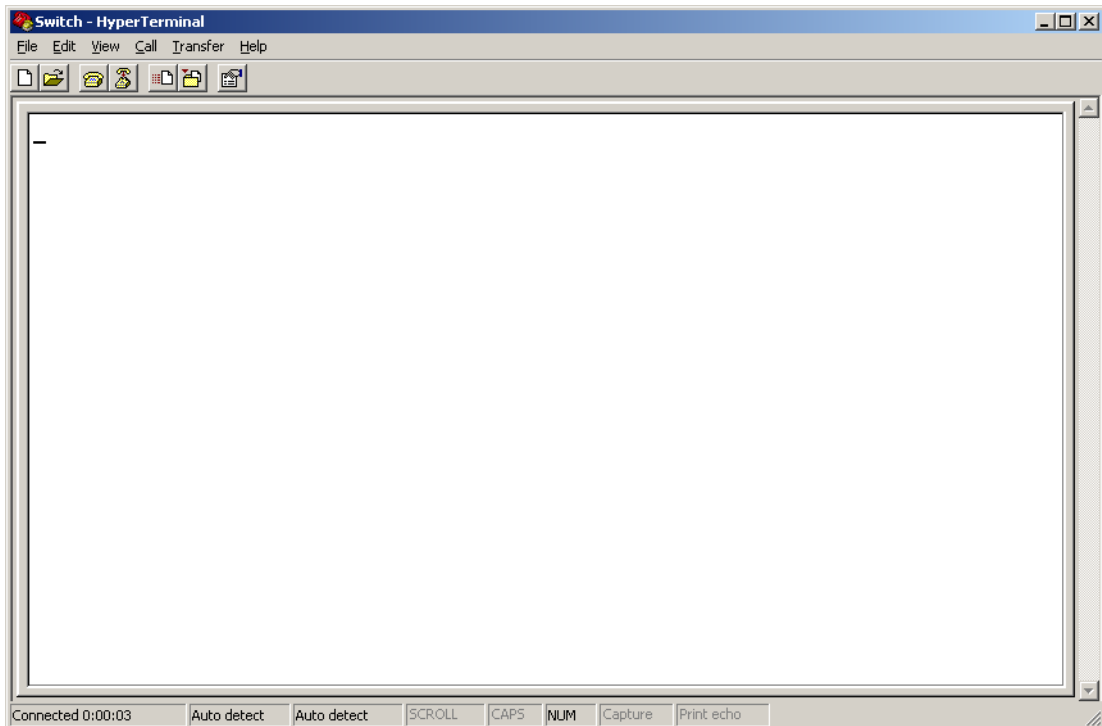
3. Set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 3 Set the serial port parameters



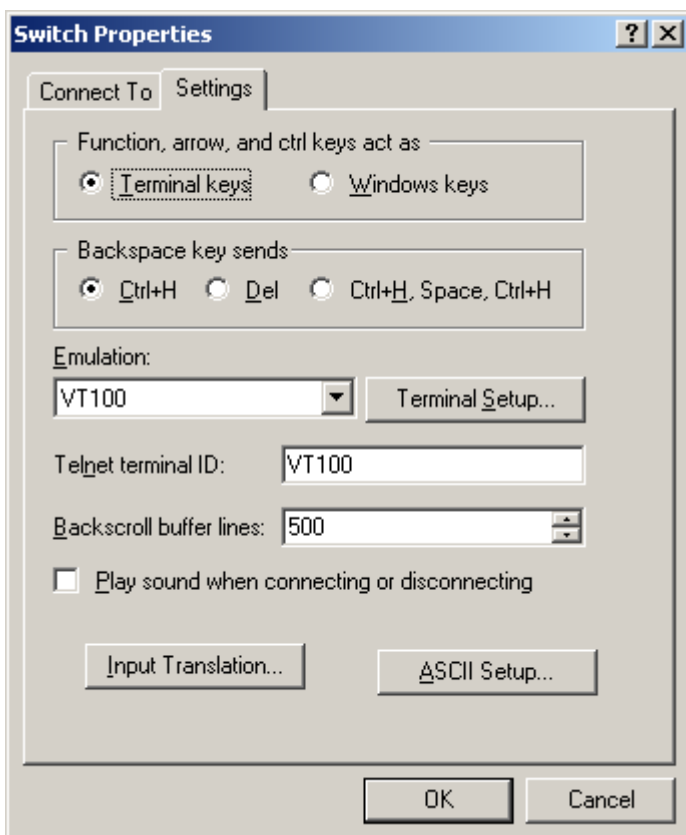
4. Select **File > Properties** in the HyperTerminal window.

Figure 4 HyperTerminal window



5. Click the **Settings** tab, set the emulation to **VT100**, and click **OK** in the **Switch Properties** dialog box.

Figure 5 Set terminal emulation in Switch Properties dialog box



Upgrading Boot ROM

Perform the following tasks to upgrade Boot ROM by using XMODEM through the console port:

1. Access the Boot menu, and enter **6** or press **Ctrl + U** to enter 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):

⚠ IMPORTANT:

Always select option **1** to upgrade the entire Boot ROM. You can use option **2** or option **3** only under the guidance of an HPE engineer.

2. Enter **1** at the Boot ROM update menu to set the protocol parameters.

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
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

Enter your choice (0-5):

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

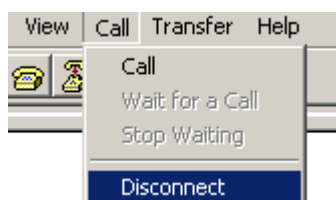
Download baudrate is 115200 bps

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

Figure 6 Disconnect the terminal from the switch



7. Select **File > Properties**. In the **Properties** dialog box, click **Configure** (see [Figure 7](#)), and then select **115200** from the **Bits per second** drop-down list box (see [Figure 8](#)).

Figure 7 Properties dialog box

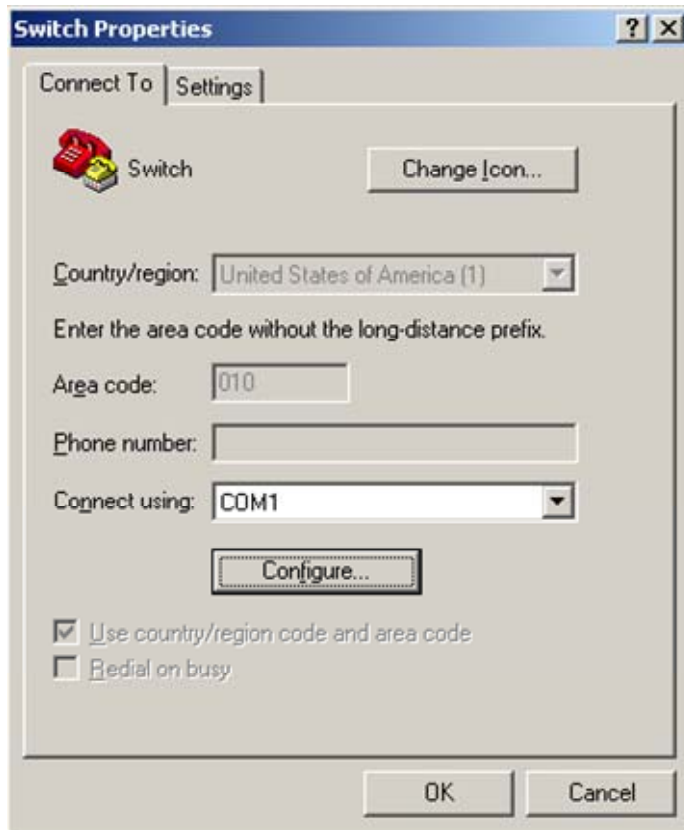
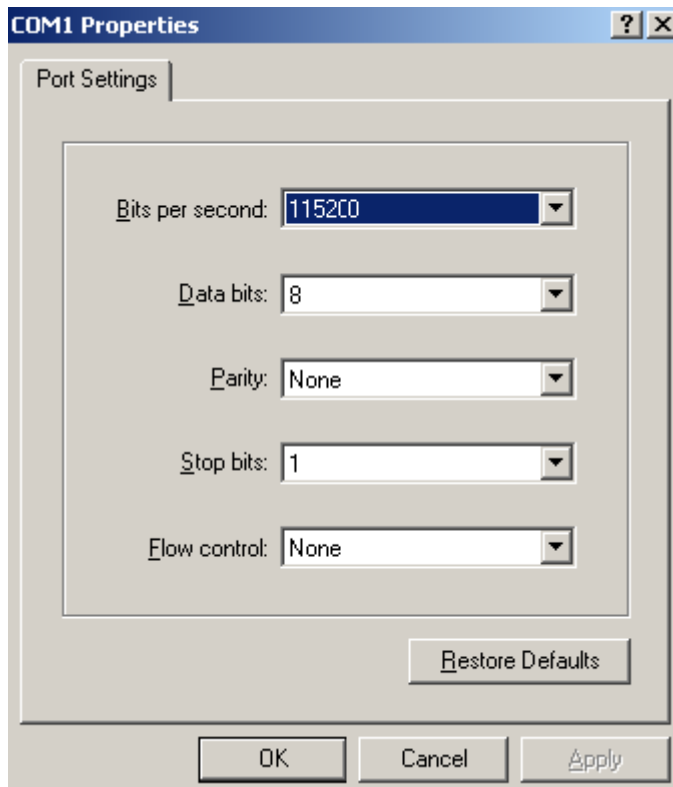
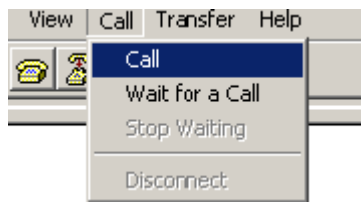


Figure 8 Modify the baud rate



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

Figure 9 Reestablish the connection



NOTE:

The new settings can take effect only after you reestablish the connection.

9. Upload the software package file from the terminal to the switch.
10. After establishing a connection between the terminal and the switch, press **Enter** in the HyperTerminal window.

Now please start transfer file with XMODEM protocol.

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

Loading ...CCCCCCCCCC

11. Select **Transfer > Send File** in the HyperTerminal window (see [Figure 10](#)), and click **Browse** in the pop-up dialog box (see [Figure 11](#)) to select the source file (for example, **update.bin**), and select **Xmodem** from the **Protocol** drop-down list.

Figure 10 Transfer menu

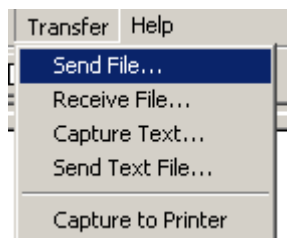
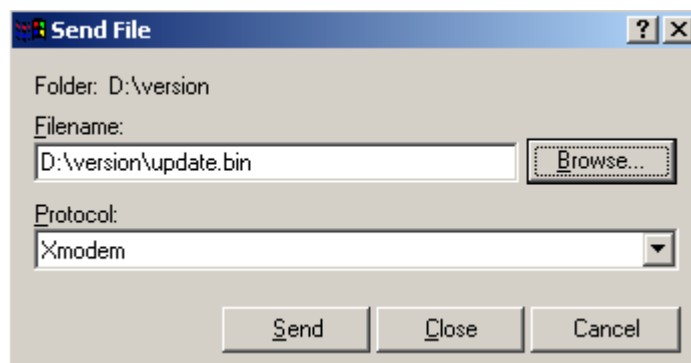
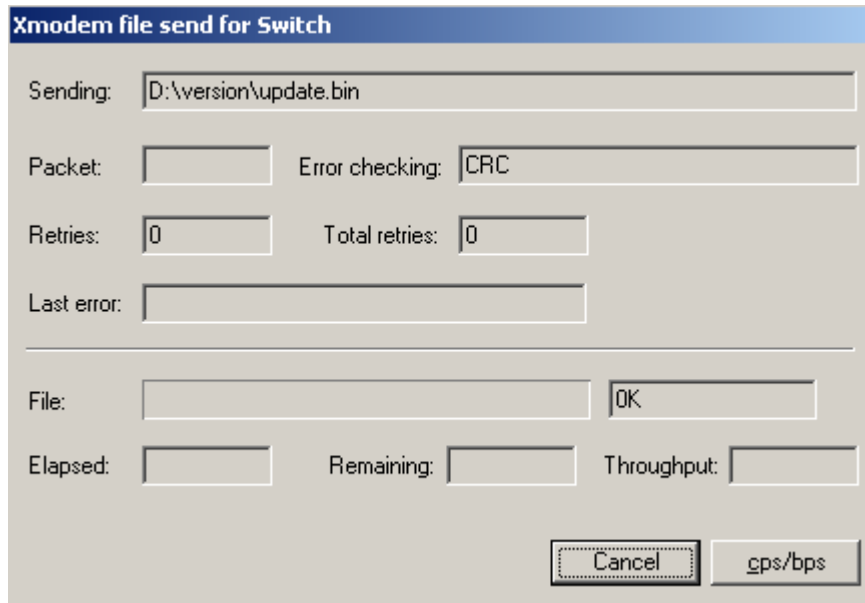


Figure 11 File transmission dialog box



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

Figure 12 Send the application file using XMODEM



13. Upgrade Boot ROM on the switch.

When the terminal displays the following prompt, enter **Y** to update the basic Boot ROM section:

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

When the terminal displays the following prompt, enter **Y** to update the extended Boot ROM section:

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

When the Boot ROM upgrade is completed, the terminal displays the following information:

```
Updating extended BootRom.....Done!  
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.
```

14. If you are using a download rate other than 9600 bps, restore the baud rate of the serial port on the terminal to 9600 bps. If the baud rate is 9600 bps, skip this step.

15. Press any key to return to the Boot ROM update menu and enter **0**. On the Boot menu that appears, enter **0** to restart the switch so the updated image can take effect. The following is 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):
```

Upgrading system software

To upgrade system software, enter **1** at the Boot menu, and the following menu appears:

```
1. Set TFTP protocol parameter  
2. Set FTP protocol parameter  
3. Set XMODEM protocol parameter  
0. Return to boot menu  
Enter your choice(0-3):3
```

Enter **3** to set the XMODEM parameters for downloading the software package file.

The subsequent procedure is the same as loading Boot ROM images, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```
Writing flash.....  
.....Done!  
Please input the file attribute (Main/Backup/None) M  
Done!
```

NOTE:

- The switch always attempts to boot first with the main file, and if the attempt fails for example, because the main file is not available, the switch tries to boot with the backup file. A file with the **none** attribute is just stored in Flash memory for backup and you must change its attribute to make it usable at reboot.
 - If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

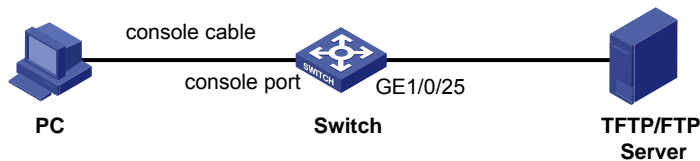
Loading Software Using TFTP through Ethernet Port

The switch can work as a TFTP client to download files from a TFTP server.

Upgrading Boot ROM

1. Connect an Ethernet port (for example, GigabitEthernet 1/0/25) of the switch to the server and connect the console port of the switch to a PC (see [Figure 13](#)).

Figure 13 Load software using TFTP/FTP through Ethernet port



NOTE:

- The PC and the TFTP/FTP server can be co-located.
 - The A5120 SI switches do not come with any TFTP server program, and you must install one yourself.
-

2. Run the TFTP server program on the server and specify the source file path.
3. Run a terminal emulator program on the PC, power on the switch, access the Boot menu, and enter **6** to access the following 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):

4. Enter **1** to upgrade the entire Boot ROM and access the following protocol parameter setting menu:

Bootrom update menu:

```
1. Set TFTP protocol parameter
```

2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):

5. Enter 1 to set the TFTP parameters.

```
Load File Name      :update.bin
Server IP Address   :10.10.10.2
Local IP Address    :10.10.10.3
Gateway IP Address :
```

Table 9 Description of the TFTP parameters

Item	Description
Load File Name :	Name of the file to be downloaded (for example, update.bin)
Server IP Address :	IP address of the TFTP server (for example, 10.10.10.2)
Local IP Address :	IP address of the switch (for example, 10.10.10.3)
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:

If the switch and the server are on different subnets, you must specify a gateway address for the switch.

6. Enter all required parameters.

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

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

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

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

When the upgrade is completed, the following information appears:

```
Updating extended BootRom.....Done!
```

7. Press any key to return to the Boot ROM update menu, enter 0 to return to the Boot menu, and enter 0 to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

```
Press enter key when ready
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu
Enter your choice(0-3):
```

Upgrading system software

To upgrade switch software, enter **1** at the Boot menu to access the following menu:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter

```
0. Return to boot menu
Enter your choice(0-3):3
```

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

The subsequent procedure of is the same as upgrading Boot ROM, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```
Writing flash.....
.....Done!
Please input the file attribute (Main/Backup/None) M
Done!
```

NOTE:

- If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

Loading Software Using FTP through Ethernet Port

The switch can work as an FTP server or FTP client to download files through an Ethernet port. This section uses the switch as an FTP client to describe the procedure.

Upgrading Boot ROM

NOTE:

When upgrading Boot ROM, the switch can work only as an FTP client.

1. Connect an Ethernet port (GigabitEthernet 1/0/25, for example) of the switch to the server and connect the console port of the switch to a PC (see [Figure 13](#)).
2. Run an FTP server program on the server, configure an FTP username and password, and specify the source file path.
3. Run a terminal emulator program on the PC, power on the switch, access the Boot menu, and enter **6** to access the following 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):
```

4. Enter **1** to upgrade the entire Boot ROM and access the following protocol parameter setting menu:

Bootrom update menu:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

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

```
Load File Name      :update.bin
Server IP Address   :10.10.10.2
Local IP Address    :10.10.10.3
```


Gateway IP Address :0.0.0.0
 FTP User Name :5120
 FTP User Password :123

Table 10 Description of the FTP parameters

Item	Description
Load File Name :	Name of the file to be downloaded (for example, update.bin)
Server IP Address :	IP address of the FTP server (for example, 10.10.10.2)
Local IP Address :	IP address of the switch (for example, 10.10.10.3)
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:

If the switch and the server are on different subnets, you must specify a gateway address for the switch.

6. Enter all required parameters.

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

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

Updating Basic BootRom.....Done!

Updating extended BootRom? (Y/N):Y

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

When the upgrade is completed, the following information appears:

Updating extended BootRom.....Done!

7. Press any key to return to the Boot ROM update menu, enter 0 to return to the Boot menu, and enter 0 to restart the switch from the Boot menu so the upgraded Boot ROM can take effect.

Press enter key when ready

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

Enter your choice(0-3):

Upgrading system software

To upgrade switch software, enter **1** in the Boot menu to access the following menu:

- 1. Set TFTP protocol parameter
- 2. Set FTP protocol parameter
- 3. Set XMODEM protocol parameter
- 0. Return to boot menu

Enter your choice(0-3):3

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

The subsequent procedure is the same as upgrading Boot ROM, except that you must set the attribute of the file as **main**, **backup**, or **none** to complete the file loading.

```

Writing flash.....
.....Done!
Please input the file attribute (Main/Backup/None) M
Done!

```

NOTE:

- If a file with the same attribute as the file you are loading is already in the Flash memory, the attribute of the old file changes to **none** after the new file becomes valid.
 - The switch automatically updates Boot ROM when loading system software.
-

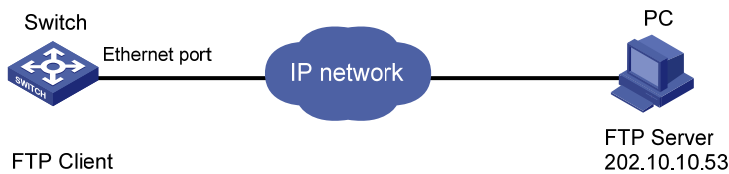
Upgrading at the CLI

You can remotely download Boot ROM and system software images at the CLI.

Loading Software Using FTP

This section uses the topology in [Figure 14](#) as an example. Run FTP server on the management PC at 202.10.10.53, create an FTP username **admin** and password, specify the source file path, telnet to the switch, and get the software package file (for example, **update.bin**) from the server.

Figure 14 FTP download from a server



1. Get the file to the switch by using FTP.

```

<HPE> ftp 202.10.10.53
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):admin
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get update.bin update.bin
[ftp] bye

```

2. Upgrade Boot ROM.

```

<HPE> bootrom update file update.bin slot 1
This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
Now updating bootrom, please wait...

```

3. Load the system software image and specify the file as the main file at the next reboot.

```

<HPE> boot-loader file update.bin slot 1 main
This command will set the boot file of the specified board. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 1!

```

```
<HPE> display boot-loader
Slot 1
The current boot app is:  flash:/update.bin
The main boot app is:    flash:/update.bin
The backup boot app is:  flash:/update.bin
<HPE> reboot
```

NOTE:

- You must reboot the switch with the **reboot** command to complete the upgrade. Before that, save the configurations you have made to avoid data loss.
 - If Flash memory is insufficient, load the Boot ROM image first and delete useless files to free up Flash memory before you load the system software image.
 - Avoid power failure during the loading process.
-

Loading Software Using TFTP

The switch can work as a TFTP client to download files from a TFTP server, and the downloading procedure is similar to downloading files through FTP. With these two protocols, the subsequent Boot ROM and system software image loading procedures are the same.