

A5120SI-CMW520-R1513P15 Release Notes

© Copyright 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information in this document is subject to change without notice.



Contents

Version information	4
Version number	4
Version history	4
Hardware and software compatibility matrix	6
Upgrading restrictions and guidelines	7
Hardware feature updates	7
A5120SI-CMW520-R1513P15	7
A5120SI-CMW520-R1513P13	8
A5120SI-CMW520-R1513P07	8
A5120SI-CMW520-F1513P06	8
A5120SI-CMW520-F1513P05	8
A5120SI-CMW520-F1513P02	8
A5120SI-CMW520-F1513P01	8
A5120SI-CMW520-F1513	8
A5120SI-CMW520-R1512P05	8
A5120SI-CMW520-R1511	8
A5120SI-CMW520-F1509	8
A5120SI-CMW520-R1505P09	9
A5120SI-CMW520-R1505P07	9
A5120SI-CMW520-R1505P06	9
A5120SI-CMW520-R1505P05	9
Software feature and command updates	9
MIB updates	9
Operation changes	11
Operation changes in R1513P15	11
Operation changes in R1513P13	11
Operation changes in R1513P07	11
Operation changes in F1513P06	11
Operation changes in F1513P05	11
Operation changes in F1513P02	11
Operation changes in F1513P01	11
Operation changes in F1513	12
Operation changes in R1512P05	12
Operation changes in R1511	12
Operation changes in F1509	12
Operation changes in R1505P09	12
Operation changes in R1505P07	12
Operation changes in R1505P06	13
Operation changes in R1505P05	13
Restrictions and cautions	13
Open problems and workarounds	13
List of resolved problems	15
Resolved problems in R1513P15	15
Resolved problems in R1513P13	15
Resolved problems in R1513P07	16

Resolved problems in F1513P06	17
Resolved problems in F1513P05	18
Resolved problems in F1513P02	18
Resolved problems in F1513P01	18
Resolved problems in F1513	19
Resolved problems in R1512P05	20
Resolved problems in R1511	20
Resolved problems in F1509	22
Resolved problems in R1505P09	26
Resolved problems in R1505P07	26
Resolved problems in R1505P06	26
Resolved problems in R1505P05	26
Related documentation	27
Documentation set	27
Obtaining documentation	27
Contacting HP	27
Subscription service	27
Appendix A Feature list	28
Hardware features	28
Switch models	28
Technical specifications	28
Software features	29
Appendix B Upgrading software	34
Upgrading software from Boot ROM menus	34
Accessing the basic Boot menu	36
Accessing the extended Boot menu	37
Loading Software Using XMODEM through Console Port	39
Loading Software Using TFTP through Ethernet Port	48
Loading Software Using FTP through Ethernet Port	51
Upgrading at the CLI	53
Loading Software Using FTP	53
Loading Software Using TFTP	54

List of Tables

Table 1 Version history	4
Table 2 HP A5120SI product family matrix	6
Table 3 Hardware and software compatibility matrix.....	6
Table 4 MIB updates	9
Table 5 Models in the HP A5120 SI Switch Series	28
Table 6 HP A5120 SI Switch Series technical specifications	28
Table 7 Software features of the A5120 SI series	29
Table 8 Approaches to loading software on the switch	34
Table 9 Shortcut keys	35
Table 10 Basic Boot ROM menu options	36
Table 11 BASIC-ASSISTANT menu options	37
Table 12 Extended Boot ROM menu options.....	38
Table 13 EXTEND-ASSISTANT menu options	39
Table 14 Description of the TFTP parameters.....	49
Table 15 Description of the FTP parameters	52

This document describes the features, restrictions and guidelines, open problems, and workarounds for version A5120SI-CMW520-R1513P15 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 A5120SI-CMW520-R1513P15 Release Notes (Software Feature Changes) and the documents listed in "[Related documentation.](#)"

Version information

Version number

Comware software, Version 5.20, Release 1513P15

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

Version history

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
CMW520-R1513P15	CMW520-R1513P13	2013-03-21	Release version	Modified feature: Enabling/disabling FIPS mode Fixes bugs.
CMW520-R1513P13	CMW520-R1513P07	2013-02-25	Release version	Fixes bugs.
CMW520-R1513P07	CMW520-F1513P06	2013-01-05	Release version	New feature: Enabling source IP conflict prompt Disabling password recovery capacity, FIPS, IPsec, IKE, Verifying the correctness and integrity of the file, Enabling log file overwrite-protection Modified feature: Modifying security commands executed in FIPS mode for CC evaluation, Modifying CLI configuration commands executed in FIPS mode for CC evaluation, Modifying login management commands executed in FIPS mode for CC evaluation, Modifying software upgrade commands executed in FIPS mode for CC evaluation, Modifying configuration file management commands executed in FIPS mode for CC evaluation, Modifying SNMP commands executed in FIPS mode for

Version number	Last version	Release date	Release type	Remarks
				CC evaluation Fixes bugs.
CMW520-F1513P06	CMW520-F1513P05	2012-11-29	Feature version	Fixes bugs.
CMW520-F1513P05	CMW520-F1513P02	2012-10-30	Feature version	Fixes bugs.
CMW520-F1513P02	CMW520-F1513P01	2012-10-19	Feature version	Fixes bugs.
CMW520-F1513P01	CMW520-F1513	2012-09-20	Feature version	New feature: Automatic configuration file backup for software downgrading, Setting the deletion delay time for SAVI Modified feature: Configuring the password for switching from a user privilege level to a higher one, Setting a password for local authentication, Configuring a password for a local user, Clearing all users from the password control blacklist, Setting the IRF link down report delay, Cluster management Fixes bugs.
CMW520-F1513	CMW520-R1512P05	2012-08-24	Feature version	New feature: MAC authentication critical VLAN Modified feature: 802.1X critical VLAN Fixes bugs.
CMW520-R1512P05	CMW520-R1511	2012-07-12	Release version	Fixes bugs.
CMW520-R1511	CMW520-F1509	2012-05-25	Release version	Fixes bugs. adds features
CMW520-F1509	CMW520-R1505P09	2012-02-20	Feature version	Fixes bugs. adds features
CMW520-R1505P09	CMW520-R1505P07	2012-06-19	Release version	Fixes bugs.
CMW520-R1505P07	CMW520-R1505P06	2011-11-22	Release version	Fixes bugs.
CMW520-R1505P06	CMW520-R1505P05	2011-10-31	Release version	Fixes bugs.
CMW520-R1505P05	None	2011-06-21	Release version	Fixes bugs.

Hardware and software compatibility matrix

Before HP A5120SI 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 HP A5120SI will be the representation to all of them in subsequent document.

Table 2 HP A5120SI product family matrix

HP A5120SI series	H3C S5120SI series
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.

Table 3 Hardware and software compatibility matrix

Item	Specifications
Product family	A5120 SI Switch Series
Hardware platform	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
	H3C S5120-20P-SI
	H3C S5120-28P-SI
Minimum memory requirements	H3C S5120-52P-SI
	H3C S5120-28P-PWR-SI
	H3C S5120-28P-HPWR-SI
	128MB
	128 MB
Minimum Flash requirements	
Boot ROM version	Version 161 (Note: Use the display version command in any view to view the version information. See Note②)
System software image file	A5120SI-CMW520-R1513P15.bin
iMC version	iMC PLAT 5.2 (E0401H02)
	iMC UAM 5.2 (E0402)
	iMC EAD 5.2 (E0402)
	iMC QoS 5.2 (E0401)

Item	Specifications
	iMC BIMS 5.2 (E0401)
	iMC TAM 5.2 (E0401)
iNode version	iNode PC 5.2 (E0402)
Remarks	None

Display the system software version and Boot ROM version of the A5120-16G SI Switch:

```
<HP>display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 1513P15 ----- Note①
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP A5120-16G SI Switch uptime is 0 week, 0 day, 0 hour, 19 minutes

HP A5120-16G 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 161 ----- Note②
[SubSlot 0] 16GE+4SFP Hardware Version is REV.A
```

Upgrading restrictions and guidelines

- A new password encryption algorithm is adopted since Release F1509. If you roll back the software from a version between F1509 and F1513P01 (not included) to a version lower than F1509, the password that has been processed by the new encryption algorithm cannot be restored, and user login may fail.
- If the configuration is saved on a switch where a software version of F1513P01 or higher is running but the software version in the startup configuration file is still lower than F1509 (not included), the switch first backs up the startup configuration file and then saves the running configuration to the startup configuration file. For example, suppose the startup configuration file is **a.cfg**. The switch first backs up **a.cfg** as **_a_bak.cfg**, and then saves the running configuration to **a.cfg**.
- After the software is upgraded to F1513P01 or higher, any **irf link-delay** value greater than 10 seconds will be set to 4 seconds (the default).

Hardware feature updates

A5120SI-CMW520-R1513P15

None

A5120SI-CMW520-R1513P13

None

A5120SI-CMW520-R1513P07

None

A5120SI-CMW520-F1513P06

None

A5120SI-CMW520-F1513P05

None

A5120SI-CMW520-F1513P02

None

A5120SI-CMW520-F1513P01

None

A5120SI-CMW520-F1513

None

A5120SI-CMW520-R1512P05

None

A5120SI-CMW520-R1511

None

A5120SI-CMW520-F1509

None

A5120SI-CMW520-R1505P09

None

A5120SI-CMW520-R1505P07

None

A5120SI-CMW520-R1505P06

None

A5120SI-CMW520-R1505P05

None

Software feature and command updates

For more information about the software feature and command update history, see A5120SI-CMW520-R1513P15 Release Notes (Software Feature Changes).

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
A5120-SI-CMW520-R1513P15			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1513P13			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1513P07			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-F1513P06			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
A5120-SI-CMW520-F1513P05			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-F1513P02			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-F1513P01			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-F1513			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1512P05			
New	rfc4502-rmon2.mib	RMON2-MIB	None
Modified	None	None	None
A5120-SI-CMW520-R1511			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-F1509			
New	hh3c-rrpp.mib	H3C-RRPP-MIB	None
	h3c-rrpp.mib		
	savi.mib	SAVI-MIB	
Modified	None	None	None
A5120-SI-CMW520-R1505P09			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1505P07			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1505P06			
New	None	None	None
Modified	None	None	None
A5120-SI-CMW520-R1505P05			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in R1513P15

None

Operation changes in R1513P13

- The maximum number of smart link groups was changed from 4 to 26.

Operation changes in R1513P07

None

Operation changes in F1513P06

None

Operation changes in F1513P05

- Changed the default state of all TCP/UDP ports from "enabled" to "disabled", including TCP ports 23 and 7547, and UDP ports 0, 68, and 1812.
- Changed the default state of the HTTP server from "enabled" to "disabled". To enable the HTTP server, use the **ip http enable** command.

Operation changes in F1513P02

- Modified the value of node hh3cUserPassword in HH3C-USER-MIB due to security concerns. When read, hh3cUserPassword always returns a zero-length OCTET STRING.

Operation changes in F1513P01

- Changed the default value for the *time* argument in the **ipv6 savi down-delay** command from 3 minutes to 30 seconds, and from non-configurable to configurable.
- Changed the maximum value for the *interval* argument in the **irf link-delay** command from 30 seconds to 10 seconds.
- Changed the default cluster state from enabled to disabled.
- Changed the Wisdom NetWork (WiNet) management as member feature from open to close.
- If the configuration is saved on a switch where a software version of F1513P01 or higher is running but the software version in the startup configuration file is still lower than F1509 (not included), the switch first backs up the startup configuration file and then saves the running configuration to the

startup configuration file. For example, suppose the startup configuration file is **a.cfg**. The switch first backs up **a.cfg** as **_a_bak.cfg**, and then saves the running configuration to **a.cfg**.

- Changes to installing a new patch on a switch where an old patch has been installed:
 - Before modification: When installing a new patch, the switch directly replaces the old patch with the new patch, without any confirmation.
 - After modification: Before installing a new patch, the switch prompts a "Another patch loaded, please uninstall it first." message to notify the user to uninstall the old patch.

Operation changes in F1513

- Operation change for whether a port leaves the critical VLAN after the silent timer expires.

After a port is assigned to the critical VLAN, the RADIUS server state changes to "blocked", and the silent timer of the RADIUS server starts (this timer is configurable and defaults to 5 minutes).

In earlier versions:

- If the port uses 802.1X authentication, it leaves the critical VLAN when the silent timer expires. If the port is configured with the **dot1x critical recovery-action** command, its leaving triggers new 802.1X authentication.

In this version:

- If the port uses 802.1X authentication, it remains in the critical VLAN when the silent timer expires. If the port is configured with the **dot1x critical recovery-action** command, the silent timer expiration triggers new 802.1X authentication.

Operation changes in R1512P05

None

Operation changes in R1511

None

Operation changes in F1509

1. The Key can be auto-generated for the SSH service.
2. The PKI certificate can be auto-generated for HTTPS service.

Operation changes in R1505P09

None

Operation changes in R1505P07

None

Operation changes in R1505P06

None

Operation changes in R1505P05

None

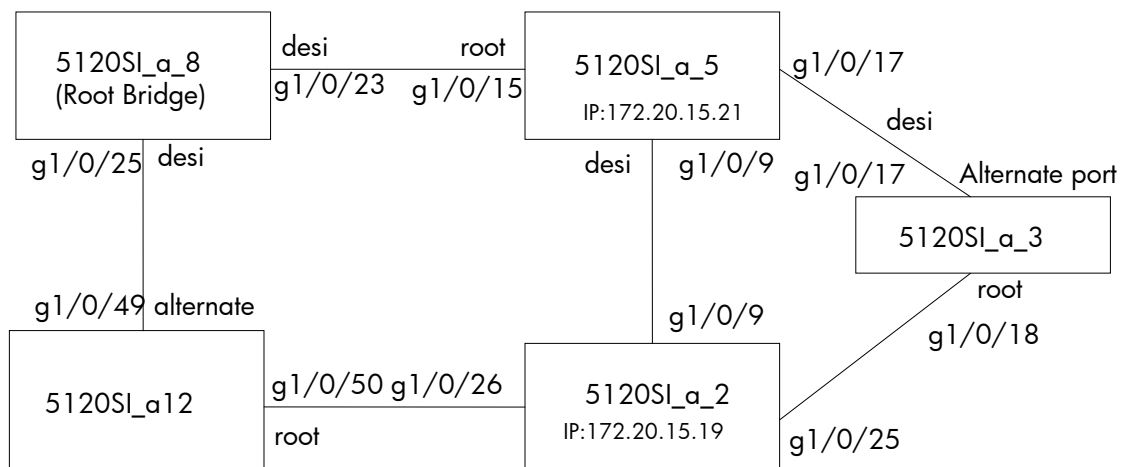
Restrictions and cautions

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 R1513P15

LSD074632

- Symptom: Global IPv6 ACLs (either manually configured or automatically assigned by a protocol) do not take effect. For example, IPv6 ACLs assigned by portal do not take effect.
- Condition: This symptom exists in R1513P13.

LSD074433

- Symptom: The memory resources are used up if many SSH connections are established using the Nessus software.
- Condition: This symptom occurs if many SSH connections are established using the Nessus software.

LSD074398

- Symptom: If the VLAN IDs specified for selective QinQ to match are not continuous (for example, **aw-vlan-id inbound 2 to 33 44 to 100**), selective QinQ can only tag an outer VLAN ID for frames from the first VLAN ID range (2 to 33 in this example).
- Condition: This symptom occurs if the VLAN IDs specified for selective QinQ to match are not continuous.

Resolved problems in R1513P13

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.

LSD074356

- Symptom: A terminal that has not passed portal authentication on the connected switch can use software such as TFTP and QQ to access the network.
- Condition: This symptom can be seen when the switch is enabled with portal authentication.

LSD73898

- Symptom: The switch does not learn MAC addresses.
- Condition: This symptom might occur when the following conditions exist:
 - CPU usage is high.
 - The MAC address table is full.
 - MAC addresses are added and deleted continually.
 - STP flapping occurs on the neighbor devices.

LSD74078

- Symptom: The service type displayed in the Web interface is different from the one configured at the CLI on the switch.
- Condition: This symptom can be seen when **service-type** has been configured in the **local-user** command.

LSD74087

- Symptom: When the idle timeout timer of a user that has logged in to the Web interface expires, an incorrect prompt "Error: Failed to set the new password!" appears.
- Condition: This symptom can be seen when the idle timeout timer of a user that has logged in to the Web interface expires.

LSD74065

- Symptom: A security-audit user cannot use the IPv6 ping and traceroute functions in the Web interface.
- Condition: This symptom occurs when a security-audit user tries to use the IPv6 ping and traceroute functions in the Web interface.

LSD074153

- Symptom: When a Web management user clicks the **Creating diagnostic information file** button in the Web interface, the switch abnormally reboots.
- Condition: This symptom occurs when a Web management user clicks the **Creating diagnostic information file** button in the Web interface.

Resolved problems in R1513P07

LSD073500

- Symptom: When a PC connected to an A5120SI switch uses the same IP address as the connected VLAN interface, the switch does not prompt address conflict.
- Condition: This symptom can be seen when a PC connected to an A5120SI switch uses the same IP address as the connected VLAN interface.

LSD073797

- Symptom: After a looped port detected by loopback-detection in multi-port mode has its loop source moved to another port, the port still cannot forward or receive packets.
- Condition: This symptom can be seen after a looped port detected by loopback-detection in multi-port mode has its loop source moved to another port.

LSD073860

- Symptom: Walking the ifOutErrors MIB node on a port always returns 0.
- Condition: This symptom might be seen when the port has incorrect packet statistics.

LSD073706

- Symptom: Disabling a port in the Web interface results in a reboot of the switch.
- Condition: This symptom might occur when you disable a port in the Web interface.

LSD073081

- Symptom: An error occurs when a user accesses the **Device -> File Management** page.
- Condition: This symptom can be seen if the user has logged in to the Web interface by using a domain name with more than 19 characters

Resolved problems in F1513P06

LSD073546

- Symptom: A terminal that matches the SNMP ACL cannot access the switch.
- Condition: This symptom occurs when a terminal that resides in the subnet permitted by the SNMP ACL tries to access the switch.

LSD073193

- Symptom: An SNMP walk on ifInErrors MIB returns a value of 0 when the interface has statistics about error packets.
- Condition: This symptom occurs when the interface has statistics about error packets.

LSD073063

- Symptom: The NTP Web page displays wrong information.
- Condition: This symptom might occur if you configure two authentication-keyids and then modify the first configured authentication-keyid.

LSD073364

- Symptom: The NDP & NTDP information displayed using the Firefox browser has font and format problems.
- Condition: This symptom occurs when you use the Firefox browser to display the NDP & NTDP information of the switch.

LSD073358

- Symptom: Prompt information displayed during LACP Web configuration has format problems.
- Condition: This symptom exists in the prompt information displayed during LACP Web configuration.

LSD072680

- Symptom: An STP Discarding port can still learn MAC addresses.
- Condition: This symptom occurs on an STP Discarding port.

HWD039649

- Symptom: When an unsupported 100M fiber module is inserted, the console does not print "not supported by hardware."
- Condition: This symptom occurs when an unsupported 100M fiber module is inserted.

HWD039650

- Symptom: The switch cannot identify 10G fiber modules. When a 10G module is inserted, the console does not print "not supported by hardware."

- Condition: This symptom occurs when a 10G module is inserted.

Resolved problems in F1513P05

LSD072694

- Symptom: An IRF fabric does not learn MAC addresses and the MAC table is empty.
- Condition: This symptom might occur if the IRF fabric frequently receives TC packets and meanwhile its MAC address table becomes full multiple times.

LSD72865

- Symptom: If a port goes down when **ipv6 savi down-delay 0** has been configured, the DHCPv6 snooping and ND snooping entries on the port are not removed.
- Condition: This symptom might occur if a port goes down when **ipv6 savi down-delay 0** has been configured.

LSD072881

- Symptom: Using the super password to switch a user privilege level fails.
- Condition: This symptom occurs if the super password is configured in irreversible mode through Web.

LSD073016

- Symptom: A string of more than four characters cannot be correctly entered into the Contact or Location box in the SNMP setup web page.
- Condition: This symptom occurs if you enter a string of more than four characters into the Contact or Location box in the SNMP setup web page.

LSD072938

- Symptom: An 802.1X-enabled port broadcasts received EAPOL-Start packets.
- Condition: This symptom might occur if 802.1X is enabled globally and on the port, and an 802.1X user has passed 802.1X authentication on the port.

Resolved problems in F1513P02

LSD073073

- Symptom: When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device returns the user's password.
- Condition: Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.

Resolved problems in F1513P01

LSD072583

- Symptom: The master in an IRF fabric might operate abnormally if a member device is rebooted multiple times after the **undo cwmp enable** command is executed on the IRF fabric.
- Condition: This symptom might occur if an IRF member device is rebooted multiple times after the **undo cwmp enable** command is executed on the IRF fabric.

LSD072548

- Symptom: If 8K DHCP clients (the full specification) continually get online and offline for about six hours through an IRF fabric that acts as the DHCP server, a member device in the IRF fabric might reboot.
- Condition: This symptom might occur if 8K DHCP clients (the full specification) continually get online and offline for about six hours through an IRF fabric that acts as the DHCP server.

LSD072441

- Symptom: A port where 802.1X authentication fails is not removed from the dot1x critical VLAN.
- Condition: This symptom might occur if the following conditions exist:
 - The port is not configured with **dot1x auth-fail vlan**.
 - The port is added to the dot1x critical VLAN when the authentication server is unreachable, but after the server is reachable, 802.1X authentication on the port fails.

LSD072436

- Symptom: The system time is incorrect after **clock timezone** and **clock summer-time** are configured, and then **undo clock timezone** and **undo clock summer-time** are configured.
- Condition: This symptom occurs after **clock timezone** and **clock summer-time** are configured, and then **undo clock timezone** and **undo clock summer-time** are configured.

LSD071787

- Symptom: If a new patch is installed on a switch that is running an old patch, the switch might operate abnormally.
- Condition: This symptom might occur if a new patch is installed on a switch that is running an old patch.

Resolved problems in F1513

LSD072043

- Symptom: The ports assigned to a critical VLAN configured with 802.1X/MAC authentication fail to be added to the critical VLAN, or are removed after added to the critical VLAN.
- Condition: This symptom might occur when multiple secondary RADIUS servers are configured on the switch and all primary and secondary servers are unreachable.

LSD65067

- Symptom: When no RADIUS server is reachable, packets sent by users in a critical VLAN trigger the switch to perform 802.1X authentication.
- Condition: This symptom might occur if the following conditions exist:
 - MAC-based 802.1X authentication is enabled.
 - The users are added to the critical VLAN because no authentication server is reachable.

LSD070321

- Symptom: The switch runs out of memory when the configuration file is restored on the **Device > Configuration** Web page.
- Condition: This symptom might occur if a configuration file that is close to or exceeds the free Flash memory is restored on the **Device > Configuration** Web page.

LSD072080

- Symptom: The switch is vulnerable to HTTP session Hijack attacks.
- Condition: This symptom might be seen when HTTP session Hijack attacks exist.

Resolved problems in R1512P05

LSD071395

- Symptom: When a 1G port is connected to a device that uses the RTL8169 network chip of RealTek, the 1G port repeatedly goes up and down.
- Condition: This symptom might occur when a 1G port is connected to a device that uses the RTL8169 network chip of RealTek.

LSD071631

- Symptom: An SCP client takes a long time to download a large file such as a .bin file.
- Condition: This symptom occurs when you use an SCP client to download a large file.

ZDD05332

- Symptom: When Avalanche injects HTTP packets to a device for a certain time, a memory leak occurs to the memory with MID 051c.
- Condition: This symptom occurs when you use Avalanche to inject HTTP packets to a device for a certain time.

Resolved problems in R1511

LSD070154

- Symptom: After the **undo snmp-agent trap enable system** command is executed, the device still outputs a CLKCHANGE trap when the system time is modified.
- Condition: This symptom occurs after you modify the system time, even if the **undo snmp-agent trap enable system** command has been executed.

LSD070191

- Symptom: IP addresses in DHCP snooping entries cannot be uploaded to the authentication server
- Condition: This symptom occurs when 802.1X authentication is configured.

LSD070324

- Symptom: After a cluster member or candidate device performs management VLAN autonegotiation through a non-hybrid cascade port, the cascade port is changed to a hybrid port that only permits the management VLAN and VLAN 1 (default).
- Condition: This symptom occurs when a cluster member or candidate device performs management VLAN autonegotiation.

LSD070260

- Symptom: If a MAC-authenticated client is moved to an unauthenticated port, the previous port does not delete the MAC authentication information of the client upon timeout.

- Condition: This symptom occurs after a MAC-authenticated client is moved to an unauthenticated port.

LSD69990

- Symptom: If the configuration file in which the configured VLANs reach the maximum number and some ACLs are configured is saved, a leak of 4% memory occurs. If the save operation is performed multiple times, the memory is used up.
- Condition:..

LSD68904

- Symptom: When a MIB test script that contains super-long variables is run, the MIB agent task is suspended.
- Condition: This symptom occurs when you run a MIB test script that contains super-long variables.

LSD69757

- Symptom: If you configure the **mac-vlan trigger enable** command when the **mac-vlan** command is not configured, a syntax-error prompt appears.
- Condition: This symptom occurs if the **mac-vlan trigger enable** command is configured when the **mac-vlan** command is not configured.

LSD69718

- Symptom: If you reboot a line card where online 802.1X users exist when the accounting-on feature is enabled, the device sends a wrong accounting-on message to the server. As a result, the server does not stop accounting for the 802.1X users that have been logged off.
- Condition: This symptom occurs if you reboot a line card where online 802.1X users exist when the accounting-on feature is enabled.

LSD69806

- Symptom: If you create link aggregation groups that have the same ID in the Web interface, the prompt information that appears is incorrect.
- Condition: This symptom occurs if you create link aggregation groups that have the same ID in the Web interface.

LSD69803

- Symptom: After you modify settings for a local user in the Web interface without entering any values for ACL, VLAN, user-profile parameters, some settings do not take effect.
- Condition: This symptom occurs after you modify settings for a local user in the Web interface without entering any values for ACL, VLAN, user-profile parameters.

LSD69826

- Symptom: After you configure authorized IP for Telnet, the authorized IP configuration only applies to VTYs 0 through 4.
- Condition: This symptom occurs after you configure authorized IP for Telnet.

LSD69861

- Symptom: The required options Mask and Next Hop in the static route Web configuration page have no red asterisks.
- Condition: This error exists in the static route Web configuration page.

LSD69862

- Symptom: After you add IPv6 equal-cost routes in the Web interface, a failure prompt appears.
- Condition: This symptom occurs after you add IPv6 equal-cost routes in the Web interface.

LSD69751

- Symptom: After a client that has passed MAC authentication is moved to an unauthenticated port, the new port cannot learn the MAC address the client, resulting in forwarding failure.
- Condition: This symptom occurs after a client that has passed MAC authentication is moved to an unauthenticated port.

LSD66665

- Symptom: After you configure packet filtering based on an ACL, modify the rule numbering step, and then delete time ranges for the ACL, the ACL rules become inactive but they are still effective.
- Condition: This symptom occurs after you configure packet filtering based on an ACL, modify the rule numbering step, and then delete time ranges for the ACL.

LSD070157

- Symptom: On a port that has learned many MAC addresses and has continuous traffic, some MAC entries might be aged out abnormally, resulting packet loss.
- Condition: This symptom might occur on a port that has learned many MAC addresses and has continuous traffic.

LSD071067

- Symptom: If you perform a warm restart or configure the **po e utilization-threshold** command when PoE is enabled, the total PoE power decreases.
- Condition: This symptom occurs if you perform a soft restart or configure the **po e utilization-threshold** command when PoE is enabled.

Resolved problems in F1509

LSD67576

- Symptom: After you configure dynamic fiber port aggregation, save the configuration, and reboot the device, all fiber ports are in Linkdown state, and the aggregation state is Unselected.
- Condition: This symptom occurs after you configure dynamic fiber port aggregation, save the configuration, and reboot the device.

LSD66700

- Symptom: After you re-assign a redirection policy to an IRF fabric and then perform a master/subordinate switchover, ACL resources among IRF member devices cannot be synchronized.
- Condition: This symptom occurs after you re-assign a redirection policy to an IRF fabric and then perform a master/subordinate switchover.

LSD66493

- Symptom: After you assign a VLAN policy on an IRF fabric to redirect traffic to a port in a slot, and then perform a master/subordinate switchover, the VLAN policy still partially takes effect.

- Condition: This symptom occurs after you assign a VLAN policy on an IRF fabric to redirect traffic to a port in a slot, and then perform a master/subordinate switchover.

LSD67569

- Symptom: After you enable the smarton feature and configure EAP authentication, clients fail to pass EAP authentication and stay in the authenticating state.
- Condition: This symptom occurs when the smarton feature and EAP authentication are configured.

ZDD04555

- Symptom: After you enable global LLDP and interface LLDP, inject LLDPUs which contain one or more unknown Organizationally Specific TLVs (not "00-80-C2", "00-12-0F" or "00-12-BB") and are larger than 500 bytes, and then display neighbor information, the device reboots abnormally.
- Condition: This symptom occurs after you enable global LLDP and interface LLDP, inject LLDPUs which contain one or more unknown Organizationally Specific TLVs (not "00-80-C2", "00-12-0F" or "00-12-BB") and are larger than 500 bytes, and then display neighbor information.

ZDD04542

- Symptom: If you inject LLDP packets in which the LCI length in the location ID TLV is 0 and then display neighbor information, the device reboots abnormally.
- Condition: This symptom occurs after you inject LLDP packets in which the LCI length in the location ID TLV is 0 and then display neighbor information.

ZDD04444

- Symptom: If you enable VTY debugging on a device and use tenet or SSH to log in to the device, the device reboots abnormally.
- Condition: This symptom occurs when you log in to a device with VTY debugging enabled.

LSD68519

- Symptom: The Electronic Label web page has no vendor information.
- Condition: This problem exists in the Electronic Label web page.

LSD68033

- Symptom: If you change an IRF interface to a none-IRF interface on an IRF fabric that comprises two switches in ring topology, the interface can receive but cannot send packets.
- Condition: This symptom occurs if you change an IRF interface to a none-IRF interface on an IRF fabric that comprises two switches in ring topology.

LSD68435

- Symptom: If huge amounts of ASCII data are sent to the VTY user interface of a switch, the switch reboots abnormally.
- Condition: This symptom might occur if huge amounts of ASCII data are sent to the VTY user interface of a switch.

LSD68135

- Symptom: If you configure **ip check** on a VLAN interface of an IRF fabric and then reboot the fabric, the previous subordinate device reboots repeatedly.
- Condition: This symptom occurs if you configure **ip check** on a VLAN interface of an IRF fabric and then reboot the fabric.

LSD66878

- Symptom: If you bind a MAC address that has been bound to a port to another port on IMC, a prompt that appears shows that the binding operation succeeds but actually the configuration fails.
- Condition: This symptom occurs if you bind a MAC address that has been bound to a port to another port on IMC.

LSD66703

- Symptom: If you configure a URL for certificate request through Web, save the configuration, and reboot the switch, the URL configuration gets lost.
- Condition: This symptom occurs if you configure a URL for certificate request through Web, save the configuration, and reboot the switch.

LSD67865

- Symptom: Garbled characters exist in the LLDP neighbor information Web page.
- Condition: This problem exists in the LLDP neighbor information Web page.

LSD67992

- Symptom: If packets with an OUI MAC as the source MAC and with a VLAN tag other than the voice VLAN are injected into a port that has static voice VLAN enabled and does not permit the voice VLAN, the port discards the injected packets.
- Condition: This symptom occurs if packets with an OUI MAC as the source MAC and with a VLAN tag other than the voice VLAN are injected into a port that has static voice VLAN enabled and does not permit the voice VLAN.

LSD67993

- Symptom: When mirroring operates normally and mirrored traffic exists, if you keep the traffic in one direction, remove the mirror group, reconfigure the group, stop the traffic in that direction, and inject traffic in the other direction, traffic mirroring fails.
- Condition: This symptom occurs if you keep the traffic in one direction, remove the mirror group, reconfigure the group, stop the traffic in that direction, and inject traffic in the other direction.

LSD68027

- Symptom: After voice traffic stops on a port where dynamic voice VLAN is enabled, the port cannot leave the voice VLAN.
- Condition: This symptom occurs after voice traffic stops on a port where dynamic voice VLAN is enabled.

LSD68513

- Symptom: CFD can output logs but cannot output traps.
- Condition: This symptom occurs when CFD is enabled.

LSD68898

- Symptom: The obtained value of the MIB variable ifPhysAddress on a Layer-2 aggregate interface is incorrect.
- Condition: This symptom occurs when you obtain the value of the MIB variable ifPhysAddress on a Layer-2 aggregate interface.

LSD69074

- Symptom: The Layer-2 aggregate interface information displayed does not include packet statistics.
- Condition: This symptom occurs when you view Layer-2 aggregate interface information.

LSD68878

- Symptom: When you add a port to an aggregation group on an IRF fabric, the prompt that appears contains useless information.
- Condition: This symptom occurs when you add a port to an aggregation group on an IRF fabric.

LSD68702

- Symptom: If you connect two ports to form a loop when MSTP is enabled, the switch reboots abnormally.
- Condition: This symptom occurs if you connect two ports to form a loop when MSTP is enabled.

LSD68724

- Symptom: If many users perform authentication repeatedly through a device where 802.1X authentication is enabled on multiple ports and portal authentication is enabled on a port, the device reboots abnormally.
- Condition: This symptom might occur if many users perform authentication repeatedly through a device where 802.1X authentication is enabled on multiple ports and portal authentication is enabled on a port.

LSD68301

- Symptom: If you repeatedly execute and remove **mac-vlan** on a port of a switch that is performing 802.1X authentication on multiple ports for different users, the switch reboots abnormally.
- Condition: This symptom might occur if you repeatedly execute and remove **mac-vlan** on a port of a switch that is performing 802.1X authentication on multiple ports for different users.

ZDD04864

- Symptom: If a user uses SSH to log into a switch that has insufficient memory resources, the switch might reboot.
- Condition: This symptom might occur if a user uses SSH to log into a switch that has insufficient memory resources.

ZDD04750

- Symptom: When the conflicted IP addresses in a DHCP address pool reach the upper limit, DHCP continuously performs address assignment, resulting in persistent 100% CPU usage.
- Condition: This symptom occurs when the conflicted IP addresses in a DHCP address pool reach the upper limit.

ZDD04705

- Symptom: If the Vendor-Specific attribute sent by the RADIUS server does not comply with the standard TLV format, the RADIUS authentication fails.
- Condition: This symptom occurs if the Vendor-Specific attribute sent by the RADIUS server does not comply with the standard TLV format.

ZDD04690

- Symptom: If multiple AAA-authenticated users telnet to a switch frequently, there is probability that only one user can log in to the switch.
- Condition: This symptom occurs if multiple AAA-authenticated users telnet to a switch frequently.

Resolved problems in R1505P09

LSD071395

- Symptom: If you connect a 1G port to a device that uses the RTL8169 network chip of RealTek. the 1G port repeatedly goes up and down.
- Condition: This symptom occurs if you connect a 1G port to a device that uses the RTL8169 network chip of RealTek.

Resolved problems in R1505P07

LSD66234

- Symptom: The transceiver cannot go up.
- Condition: Insert a non-HP transceiver and connect the fiber.

Resolved problems in R1505P06

LSD65695

- Symptom: An SFP port working in auto-negotiation mode cannot go up or has ever-increasing abort input errors.
- Condition: This symptom occurs when an SFP port works in auto-negotiation mode.

LSD65692

- Symptom: When a portal-free rule is configured for portal authentication, a free IP address is configured for Dot1X authentication, and no VLAN interface is configured for the user access VLAN, a user cannot access the network identified by the portal-free rule or the TCP port 80 of the free IP address.
- Condition: This symptom occurs when a portal-free rule is configured for portal authentication, a free IP address is configured for Dot1X authentication, and no VLAN interface is configured for the user access VLAN.

Resolved problems in R1505P05

This is the first release version.

Related documentation

Documentation set

- *HP 5120 EI & 5120 SI Switch Series Installation Guide-6W102*
- *HP 5120 SI Switch Series Configuration Guides -Release 1505-6W102*
- *HP 5120 SI Switch Series Command References -Release 1505-6W102*

Obtaining documentation

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- Select **Product Support & Troubleshooting**.
- Enter product name/number OR select the automatic product name/number detection OR select a product category.
- From the product page, choose **Manuals** to see the documentation associated with your product.

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Appendix A Feature list

Hardware features

Switch models

Table 5 Models in the HP A5120 SI Switch Series

Product code	HP description	Alias
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 6 HP A5120 SI Switch Series technical specifications

Item	Description
Physical dimensions (H x W x D)	43.6 x 440 x 160 mm (1.72 x 17.32 x 6.30 in.) (A5120-16G SI)
	43.6 x 440 x 160 mm (1.72 x 17.32 x 6.30 in.) (A5120-24G SI)
	43.6 x 440 x 260 mm (1.72 x 17.32 x 10.24 in.) (A5120-48G SI)
	43.6 x 440 x 420 mm (1.72 x 17.32 x 16.54 in.) (A5120-24G-PPoE+ SI)
	43.6 x 440 x 420 mm (1.72 x 17.32 x 16.54 in.) (A5120-24G-PoE+ SI)
Weight	≤ 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)
Console port	1

Service ports	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)
Input voltage	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 HP only, with the rated voltage ranging from -52 VDC to -55 VDC Only A5120-24G-PoE+ SI supports RPS DC input.
Power consumption (full configuration)	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) (A5120-24G-PoE+ SI) DC power input: 832 W (92 W for system power consumption and 740 W for PoE power consumption) (A5120-24G-PoE+ SI)
Operating temperature	0°C to 45°C (32°F to 113°F)
Operating humidity (noncondensing)	10% to 90%

Software features

Table 7 Software features of the A5120 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

Category	Features
	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 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

Category	Features
	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 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

Category	Features
	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 FTIPv6 TFTP TFTIPv6
Management	CLI configuration Remote configuration through Telnet Telnetv6 Console port SNMP SNMP v6 Remote Monitoring (RMON) alarm, event and history recording DM NMS 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 8 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

*****
*                                                                 *
*                HP A5120-48G SI Switch BOOTROM, Version 160    *
*                                                                 *
*****C
copyright (c) 2004-2012 Hangzhou H3C Technologies Co., Ltd.

Creation Date       : Dec 21 2012
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 9 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 160
*
*
*
*
*****

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 10 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 .

Option	Task
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 11 BASIC-ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.
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 A5120SI-CMW520-R1513P07 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 12 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 1513P07 version (or higher) for upgrade.</p>
2. Select application file to boot	<p>Specify the main and backup system software images for the next startup:</p> <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 R1513P07 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	<p>Delete the current next-startup configuration files and restore the factory-default configuration.</p> <p>This option is available only if password recovery capability is disabled.</p>
6. Enter BootRom upgrade menu	<p>Access the Boot ROM upgrade menu.</p> <p>If password recovery capability is enabled, you can upgrade the Boot ROM to any version.</p> <p>If password recovery capability is disabled, you can upgrade the Boot ROM to only Version 160 or higher.</p>
7. Skip current system configuration	<p>Start the switch without loading any configuration file.</p> <p>This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option.</p> <p>This option is available only if password recovery capability is enabled.</p>
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.

Option	Tasks
Ctrl+P: Skip Super Password	<p>Load the next-startup configuration file with all user privilege passwords configured with the super password command ignored.</p> <p>This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option.</p> <p>This option is available only if password recovery capability is enabled.</p>
Ctrl+R: Download application to SDRAM and Run	<p>Download a system software image and start the switch with the image.</p> <p>This option is available only if password recovery capability is enabled.</p>
Ctrl+Z: Access EXTEND-ASSISTANT MENU	<p>Access the EXTEND-ASSISTANT menu.</p> <p>For options in the menu, see Table 13.</p>

Table 13 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.

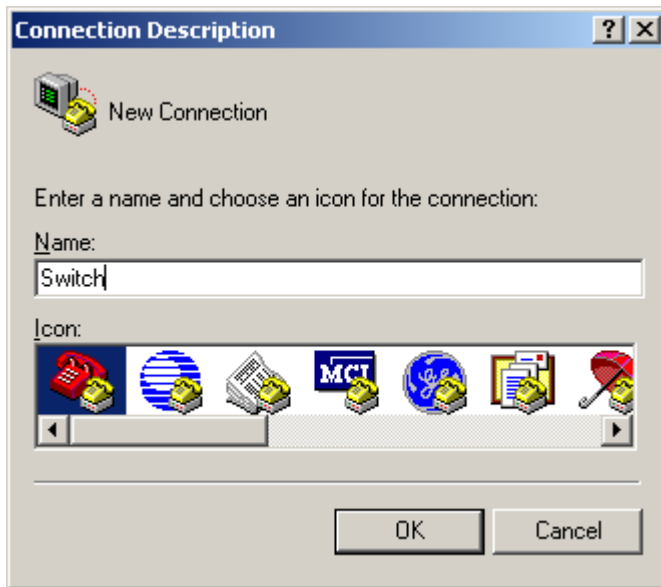
The following are the required terminal settings:

- 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:

- Step 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



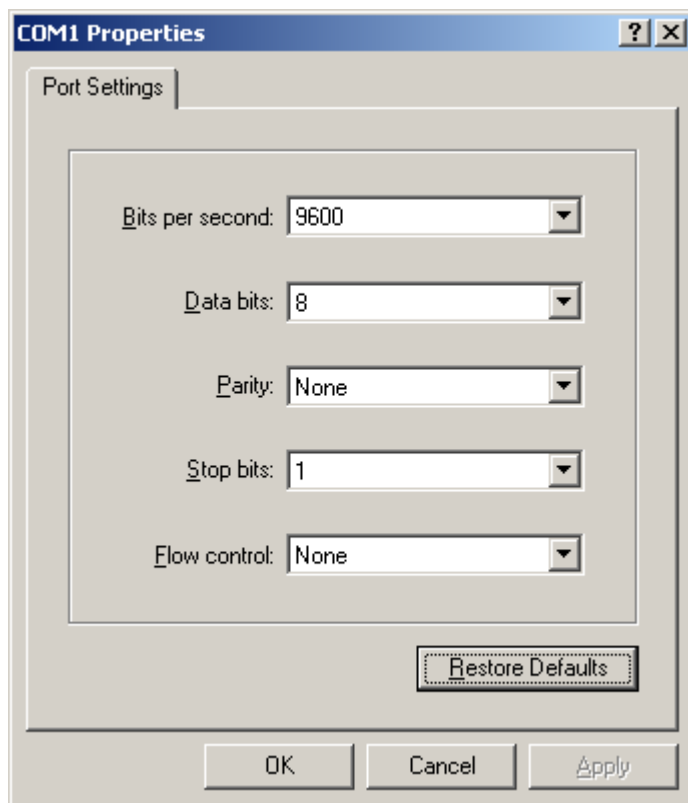
Step2 Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

Figure 2 Set the serial port used by the HyperTerminal connection



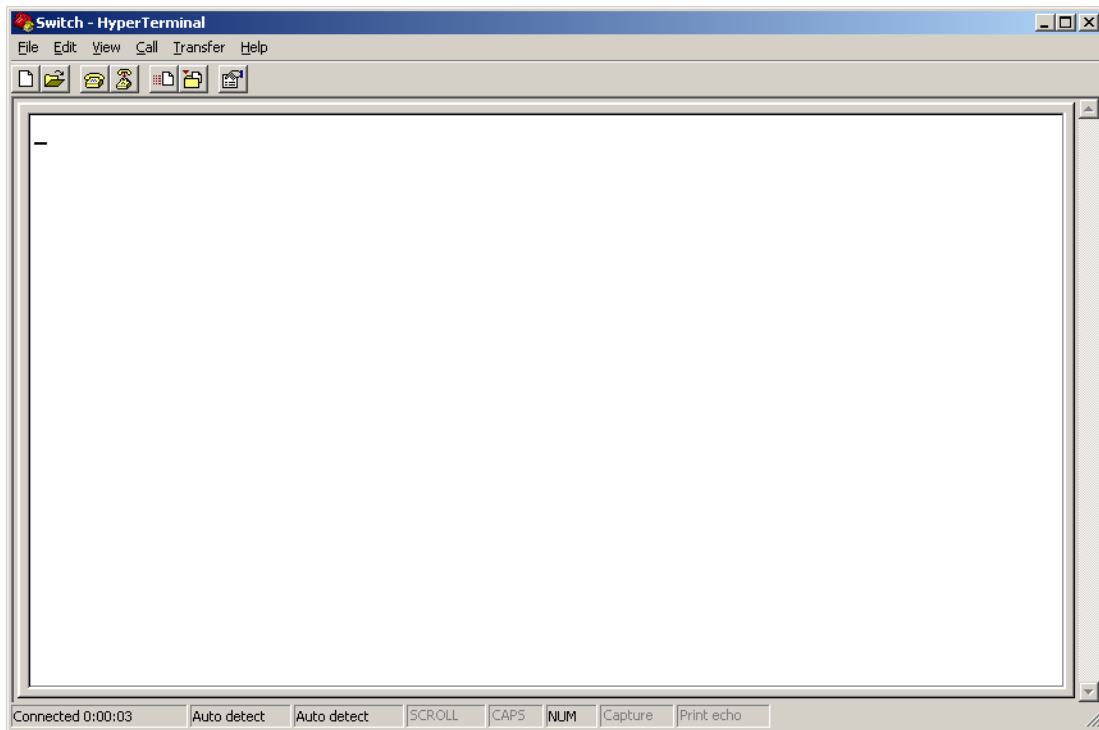
Step3 Set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 3 Set the serial port parameters



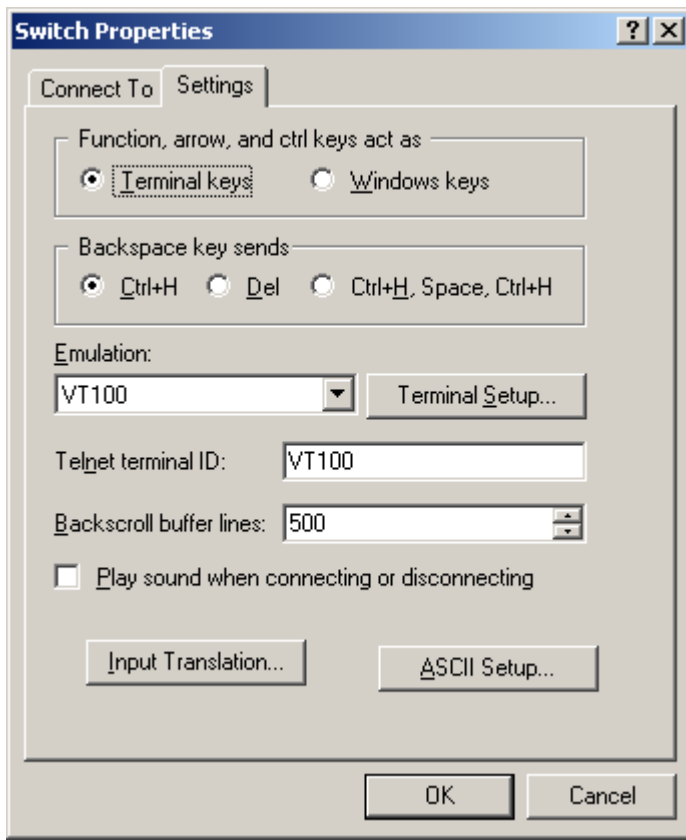
Step4 Select **File > Properties** in the HyperTerminal window.

Figure 4 HyperTerminal window



Step5 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 HP 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

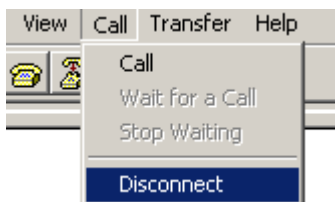
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

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.

Step1 Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 6 Disconnect the terminal from the switch



Step2 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

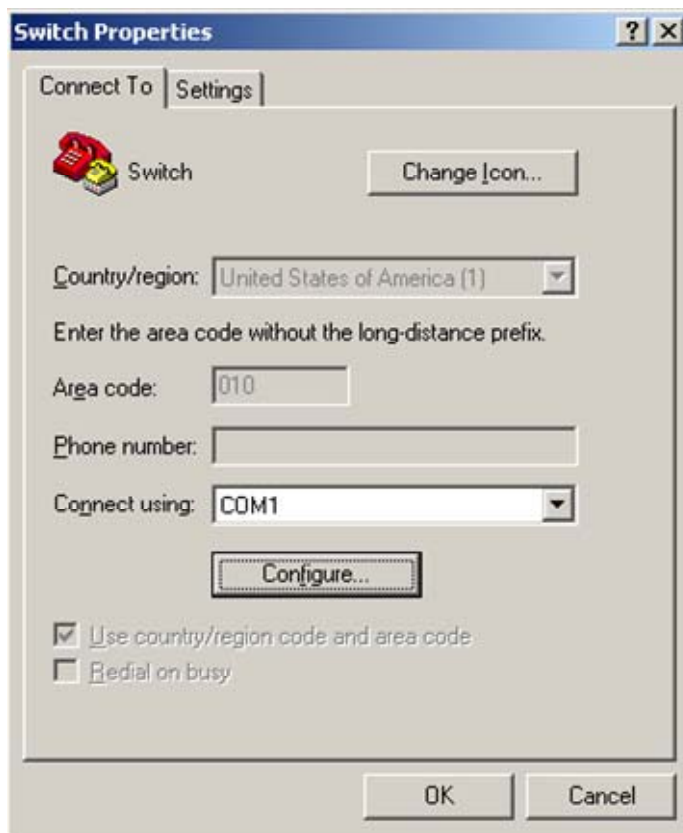
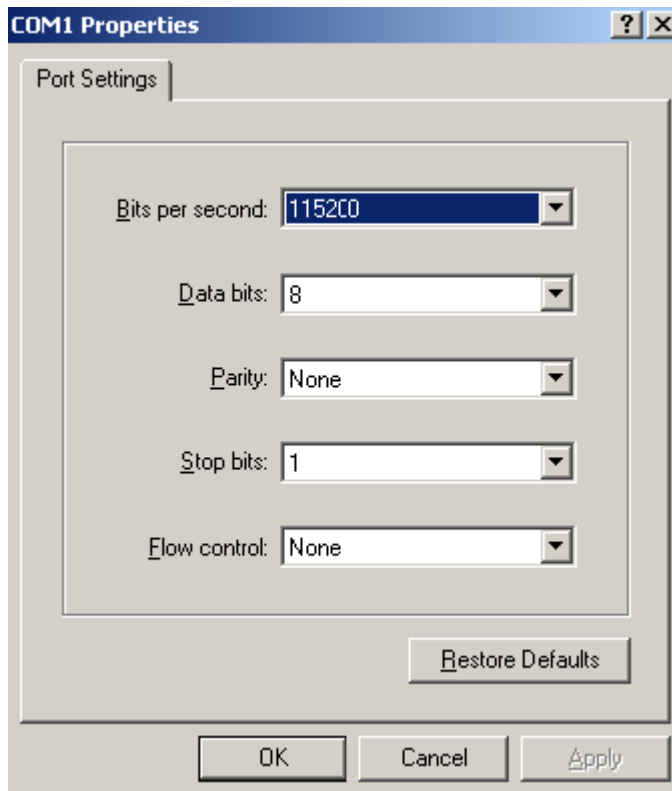
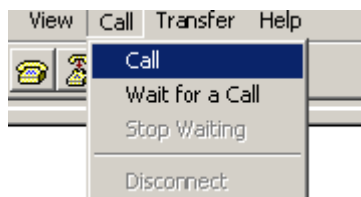


Figure 8 Modify the baud rate



Step3 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.

6. Upload the software package file from the terminal to the switch.

Step4 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

Step5 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

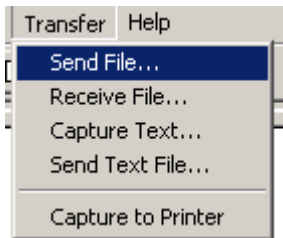
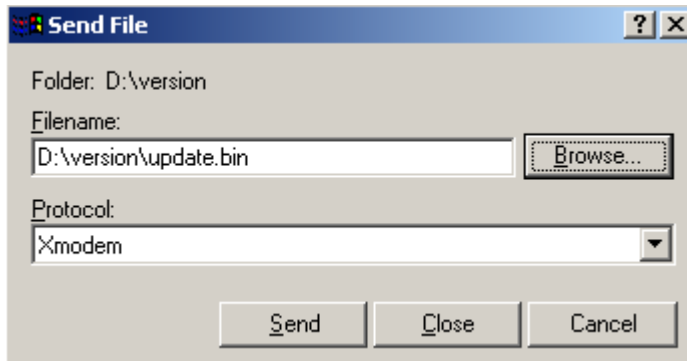
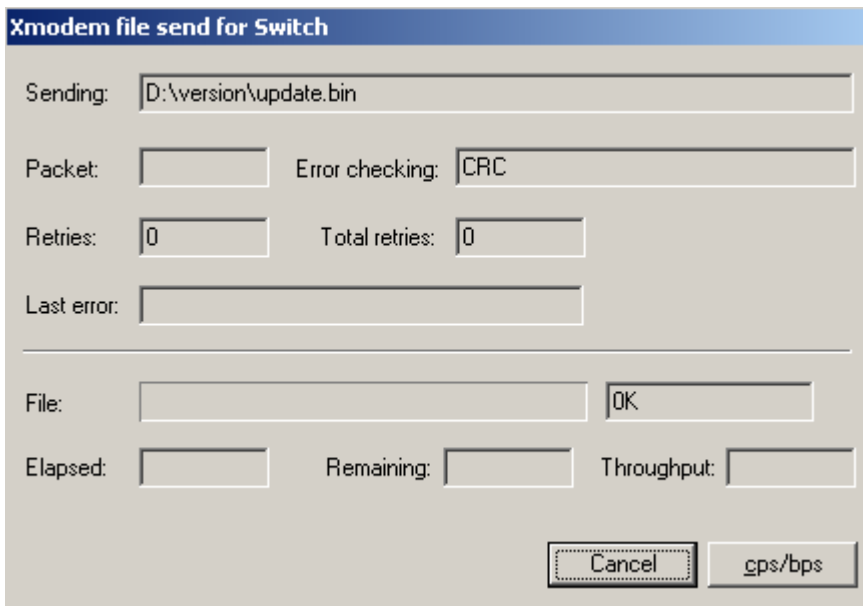


Figure 11 File transmission dialog box



Step6 Click **Send**. The following dialog box appears:

Figure 12 Send the application file using XMODEM



7. 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.
```

8. 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.
9. 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 menuEnter 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.
-

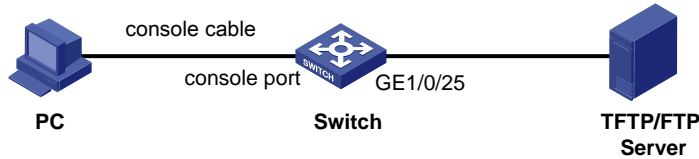
Loading Software Using TFTP through Ethernet Port

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 14 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)

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:

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 15 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.
-

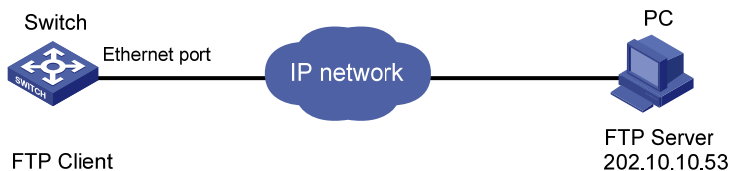
Upgrading at the CLI

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



Step1 Get the file to the switch by using FTP.

```

<HP> 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

```

Step2 Upgrade Boot ROM.

```

<HP> 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...

```

Step3 Load the system software image and specify the file as the main file at the next reboot.

```
<HP> 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!
<HP> 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
<HP> 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.