V1910-CMW520-R1515 Release Notes

© Copyright 2015 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 1
- Version number 1
- Version history 1
- Hardware and software compatibility matrix 3
- Upgrading restrictions and guidelines 5

Hardware feature updates 5
- V1910-CMW520-R1515 5
- V1910-CMW520-R1513P99 5
- V1910-CMW520-R1513P98 5
- V1910-CMW520-R1513P97 6
- V1910-CMW520-R1513P95 6
- V1910-CMW520-R1513P89 6
- V1910-CMW520-R1513P85 6
- V1910-CMW520-R1513P81 6
- V1910-CMW520-R1513P66 6
- V1910-CMW520-R1513P62 6
- V1910-CMW520-R1513P51 6
- V1910-CMW520-R1513P50 6
- V1910-CMW520-R1513P15 6
- V1910-CMW520-R1513P13 7
- V1910-CMW520-R1513P07 7
- V1910-CMW520-R1513P06 7
- V1910-CMW520-R1513P05 7
- V1910-CMW520-R1513P01 7
- V1910-CMW520-R1513 7
- V1910-CMW520-R1512P10 7
- V1910-CMW520-R1512P05 7
- V1910-CMW520-R1511 7
- V1910-CMW520-F1510 7
- V1910-CMW520-R1112 8
- V1910-CMW520-R1111P02 8
- V1910-CMW520-R1111P01 8
- V1910-CMW520-R1111 8
- V1910-CMW520-R1109 8
- V1910-CMW520-R1108P01 8
- V1910-CMW520-R1108 8

Software feature and command updates 8

MIB updates 8

Operation changes 11
- Operation changes in CMW-R1515 11
- Operation changes in CMW-R1513P99 11
- Operation changes in CMW-R1513P98 11
- Operation changes in CMW-R1513P97 11
- Operation changes in CMW-R1513P95 12
- Operation changes in CMW-R1513P89 12
- Operation changes in CMW-R1513P85 12
- Operation changes in CMW-R1513P81 12

Operation changes in CMW-R1513P66 12
Operation changes in CMW-R1513P62 12
Operation changes in CMW-R1513P51 12
Operation changes in CMW-R1513P50 12
Operation changes in CMW-R1513P15 12
Operation changes in CMW-R1513P13 13
Operation changes in CMW-R1513P07 13
Operation changes in CMW-R1513P06 13
Operation changes in CMW-R1513P05 13
Operation changes in CMW-R1513P01 13
Operation changes in CMW-R1513 13
Operation changes in CMW-R1512P10 13
Operation changes in CMW-R1512P05 13
Operation changes in CMW-R1511 14
Operation changes in CMW-F1510 14
Operation changes in CMW-R1112 14
Operation changes in CMW-R1111P02 14
Operation changes in CMW-R1111P01 14
Operation changes in CMW-R1111 14
Operation changes in CMW-R1109 14
Operation changes in CMW-R1108P01 14
Operation changes in CMW-R1108 14

Restrictions and cautions 15

Open problems and workarounds 15

List of resolved problems 16
Resolved problems in R1515 16
Resolved problems in R1513P99 17
Resolved problems in R1513P98 18
Resolved problems in R1513P97 18
Resolved problems in R1513P95 19
Resolved problems in R1513P89 21
Resolved problems in CMW520-R1513P85 21
Resolved problems in CMW520-R1513P81 22
Resolved problems in CMW520-R1513P66 22
Resolved problems in CMW520-R1513P62 22
Resolved problems in CMW520-R1513P51 22
Resolved problems in CMW520-R1513P50 23
Resolved problems in CMW520-R1513P15 23
Resolved problems in CMW520-R1513P13 24
Resolved problems in CMW520-R1513P07 25
Resolved problems in CMW520-R1513P06 25
Resolved problems in CMW520-R1513P05 26
Resolved problems in CMW520-R1513P01 27
Resolved problems in CMW520-R1513 27
Resolved problems in CMW520-R1512P10 28
Resolved problems in CMW520-R1512P05 28
Resolved problems in CMW520-R1511 28
Resolved problems in CMW520-F1510 28
Resolved problems in CMW520-R1112 28
Resolved problems in CMW520-R1111P02 30
Resolved problems in CMW520-R1111P01 30
Resolved problems in CMW520-R1111 30
Resolved problems in CMW520-R1109 31

Resolved problems in CMW520-R1108P01 32
Resolved problems in CMW520-R1108 32

Related documentation 32
Documentation set 32
Obtaining documentation 33

Contacting HP 33
Subscription service 33

Appendix A Feature list 34
Hardware features 34
Software features 35

Appendix B Upgrading software 38
Upgrading software from Boot ROM menus 38
Accessing the basic Boot menu 40
Accessing the extended Boot menu 41
Loading Software Using XMODEM through Console Port 43
Loading Software Using TFTP through Ethernet Port 52
Loading Software Using FTP through Ethernet Port 55
Upgrading at the CLI 57
Loading Software Using TFTP 57

List of Tables

Table 1 Version history 1
Table 2 HP 1910 product family matrix 3
Table 3 Hardware and software compatibility matrix 4
Table 4 MIB updates 8
Table 5 1910 series hardware features 34
Table 6 Software features of the V1910 series 35
Table 7 Approaches to loading software on the switch 38
Table 8 Shortcut keys 39
Table 9 Basic Boot ROM menu options 40
Table 10 BASIC-ASSISTANT menu options 41
Table 11 Extended Boot ROM menu options 42
Table 12 EXTEND-ASSISTANT menu options 43
Table 13 Description of the TFTP parameters 53
Table 14 Description of the FTP parameters 55

This document describes the features, restrictions and guidelines, open problems, and workarounds for version V1910-CMW520-R1515. 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 *V1910-CMW520-R1515 Release Notes (Software Feature Changes)* and the documents listed in "Related documentation."

Version information

Version number

Comware software, Version 5.20, Release 1515

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

Version history

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
V1910-CMW520-R1515	V1910-CMW520-R1513P99	2015-08-28	Release version	Fixes bugs.
V1910-CMW520-R1513P99	V1910-CMW520-R1513P98	2015-06-29	Release version	Fixes bugs.
V1910-CMW520-R1513P98	V1910-CMW520-R1513P97	2015-05-30	Release version	Fixes bugs.
V1910-CMW520-R1513P97	V1910-CMW520-R1513P95	2015-04-30	Release version	• New feature: AutoConfig • Fixes bugs.
V1910-CMW520-R1513P95	V1910-CMW520-R1513P89	2015-01-30	Release version	Fixes bugs.
V1910-CMW520-R1513P89	V1910-CMW520-R1513P85	2014-10-20	Release version	Fixes bugs.
V1910-CMW520-R1513P85	V1910-CMW520-R1513P81	2014-04-02	Release version	Fixes bugs.
V1910-CMW520-R1513P81	V1910-CMW520-R1513P66	2013-11-19	Release version	Fixes bugs.
V1910-CMW520-R1513P66	V1910-CMW520-R1513P62	2013-09-22	Release version	• New feature: Configuring an NTP polling interval • Fixes bugs.

Version number	Last version	Release date	Release type	Remarks
V1910-CMW520-R1513P62	V1910-CMW520-R1513P51	2013-09-02	Release version	• New feature: Configuring GTS on a port Establishing a Telnet connection • Fixes bugs.
V1910-CMW520-R1513P51	V1910-CMW520-R1513P50	2013-06-20	Release version	Fixes bugs.
V1910-CMW520-R1513P50	V1910-CMW520-R1513P15	2013-05-23	Release version	Fixes bugs.
V1910-CMW520-R1513P15	V1910-CMW520-R1513P13	2013-03-21	Release version	Fixes bugs.
V1910-CMW520-R1513P13	V1910-CMW520-R1513P07	2013-02-25	Release version	• Modified feature: Upgrading the PoE software from the CLI • Fixes bugs.
V1910-CMW520-R1513P07	V1910-CMW520-R1513P06	2013-01-05	Release version	Fixes bugs.
V1910-CMW520-R1513P06	V1910-CMW520-R1513P05	2012-11-29	Release version	Fixes bugs.
V1910-CMW520-R1513P05	V1910-CMW520-R1513P01	2012-10-30	Release version	Fixes bugs.
V1910-CMW520-R1513P01	V1910-CMW520-R1513	2012-10-19	Release version	Fixes bugs.
V1910-CMW520-R1513	V1910-CMW520-R1512P10	2012-09-20	Release version	• New feature: Automatic configuration file backup for software downgrading, Configuring IPv6 • Modified feature: Configuring a local user, Setting the super password, Creating users • Fixes bugs.
V1910-CMW520-R1512P10	V1910-CMW520-R1512P05	2012-08-24	Release version	Fixes bugs.
V1910-CMW520-R1512P05	V1910-CMW520-R1511	2012-07-12	Release version	Fixes bugs.
V1910-CMW520-R1511	V1910-CMW520-F1510	2012-5-25	Release version	Fixes bugs. adds features
V1910-CMW520-F1510	V1910-CMW520-R1112	2012-5-14	Feature version	Fixes bugs. adds features

Version number	Last version	Release date	Release type	Remarks
V1910-CMW520-R1112	V1910-CMW520-R1111P01	2012-4-11	Release version	Fixes bugs.
V1910-CMW520-R1111P02	V1910-CMW520-R1111P01	2012-6-19	Release version	Fixes bugs.
V1910-CMW520-R1111P01	V1910-CMW520-R1111	2012-3-20	Release version	Fixes bugs.
V1910-CMW520-R1111	V1910-CMW520-R1109	2012-1-4	Release version	Fixes bugs.
V1910-CMW520-R1109	V1910-CMW520-R1108P01	2011-9-26	Release version	Fixes bugs. adds features
V1910-CMW520-R1108P01	V1910-CMW520-R1108	2011-8-17	Release version	Fixes bugs.
V1910-CMW520-R1108	None	2011-5-13	Release version	Fixes bugs.

Hardware and software compatibility matrix

Please note that prior to October 2011, these products were shipped under the 3Com Baseline Plus 2900 series brand. The table below shows the mapping between the 3Com 2900 models and HP 1910 switches. Please note that the products are identical except for the branding. HP recommends that customers upgrade to the latest version of software to avail of the new software branding.

Table 2 HP 1910 product family matrix

HP 1910	3Com 2900
1910-16G : JE005A	3Com Baseline Plus Switch 2920
1910-24G : JE006A	3Com Baseline Plus Switch 2928
1910-24G-PoE (365W) : JE007A	3Com Baseline Plus Switch 2928 HPWR
1910-24G-PoE (170W) : JE008A	3Com Baseline Plus Switch 2928 PWR
1910-48G : JE009A	3Com Baseline Plus Switch 2952
1910-8G : JG348A	---
1910-8G-PoE+ (65W) : JG349A	---
1910-8G-PoE+ (180W) : JG350A	---

CAUTION:

To avoid an upgrade failure, use Table 4 to verify the hardware and software compatibility before performing an upgrade.

Table 3 Hardware and software compatibility matrix

Item	Specifications
Product family	HP 1910 Switch series
Hardware platform	HP1910-16G : JE005A HP 1910-24G : JE006A HP 1910-24G-PoE (365W) : JE007A HP 1910-24G-PoE (170W) : JE008A HP 1910-48G : JE009A HP 1910-8G : JG348A HP 1910-8G-PoE+ (65W) : JG349A HP 1910-8G-PoE+ (180W) : JG350A
Memory	128 MB
Flash	128 MB
Boot ROM version	Version 173(Note: Perform the **summary** command in any view to view the version information. See Note②)
Host software	V1910-CMW520-R1515.bin
iMC version	iMC EAD 7.1 (E0301P03) iMC UAM 7.1 (E0302P08) iMC PLAT 7.1 (E0303P10) iMC QoSM 7.1 (E0301P01)
iNode version	iNode PC 7.1 (E0307)
Remarks	None

```
<HP V1910 Switch>summary
Select menu option:             Summary
IP Method:                      Manual
IP address:                     192.168.1.22
Subnet mask:                    255.255.255.0
Default gateway:

Current boot app is: flash:/V1910-CMW520-R1515.bin
Next main boot app is: flash:/v1910-cmw520-R1511.bin
Next backup boot app is: NULL

HP Comware Platform Software
Comware Software, Version 5.20 Release 1515,       ------- Note①
Copyright (c) 2004-2013 Hewlett-Packard Development Company, L.P.
HP V1910-48G Switch uptime is 0 week, 0 day, 0 hour, 33 minutes

HP V1910-48G Switch
128M    bytes DRAM
128M    bytes Nand Flash Memory
Config Register points to Nand Flash
```

```
Hardware Version is REV.B
CPLD Version is 002
Bootrom Version is 173                          ------ Note②
[SubSlot 0] 48GE+4SFP Hardware Version is REV.B
```

Upgrading restrictions and guidelines

- A new password encryption algorithm is adopted since Release F1510. If you roll back the software from a version between F1510 and F1513P01 (not included) to a version lower than F1510, 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 R1513 or higher is running but the software version in the startup configuration file is still lower than F1510 (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 an upgrade from an old version to a version between R1109 and F1513P01, the system.xml configuration becomes invalid.
- After an upgrade from a version between R1109 and R1513P01 to R1513P05 or later, the system.xml configuration file is preferred by the system.
- After a downgrade from R1513P05 or later to R1108P01 or before, you must reconfigure idle timeout, syslog buffer, ntp server1, and ntp server2 in the web interface.
- In compliance with FIPS, the switch verifies the startup software image and the Boot ROM image when you execute the **boot-loader** and **bootrom update** commands on R1513P89 or later. On R1513P89 or later, the commands cannot specify a version earlier than R1509. To downgrade software to R1509 or earlier, first downgrade software to a version between R1509 and R1513P89.

Hardware feature updates

V1910-CMW520-R1515

None

V1910-CMW520-R1513P99

None

V1910-CMW520-R1513P98

None

V1910-CMW520-R1513P97

None

V1910-CMW520-R1513P95

None

V1910-CMW520-R1513P89

None

V1910-CMW520-R1513P85

None

V1910-CMW520-R1513P81

None

V1910-CMW520-R1513P66

None

V1910-CMW520-R1513P62

None

V1910-CMW520-R1513P51

None

V1910-CMW520-R1513P50

None

V1910-CMW520-R1513P15

None

V1910-CMW520-R1513P13

None

V1910-CMW520-R1513P07

None

V1910-CMW520-R1513P06

None

V1910-CMW520-R1513P05

None

V1910-CMW520-R1513P01

None

V1910-CMW520-R1513

None

V1910-CMW520-R1512P10

None

V1910-CMW520-R1512P05

None

V1910-CMW520-R1511

None

V1910-CMW520-F1510

Support new devices 1910-8G , 1910-8G-PoE+ (65W) and 1910-8G-PoE+ (180W)

V1910-CMW520-R1112

None

V1910-CMW520-R1111P02

None

V1910-CMW520-R1111P01

None

V1910-CMW520-R1111

None

V1910-CMW520-R1109

None

V1910-CMW520-R1108P01

None

V1910-CMW520-R1108

None

Software feature and command updates

For more information about the software feature and command update history, see *V1910-CMW520-R1515 Release Notes (Software Feature Changes)*.

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
V1910-CMW520-R1515			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
V1910-CMW520-R1513P99			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P98			
New	None	None	None
Modified	rfc4293-ip.mib	IP-MIB	Changed the access attribution by the following MIBs from read-write to read-only: ipForwarding ipDefaultTTL
V1910-CMW520-R1513P97			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P95			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P89			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P85			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P81			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P66			
New	rfc2674-qbridge.mib	Q-BRIDGE-MIB	None
Modified	None	None	None
V1910-CMW520-R1513P62			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P51			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P50			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
V1910-CMW520-R1513P15			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P13			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P07			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P06			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P05			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513P01			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1513			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1512P10			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1512P05			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1511			
New	None	None	None
Modified	None	None	None
V1910-CMW520-F1510			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1112			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
V1910-CMW520-R1111P02			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1111P01			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1111			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1109			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1108P01			
New	None	None	None
Modified	None	None	None
V1910-CMW520-R1108			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in CMW-R1515

None

Operation changes in CMW-R1513P99

None

Operation changes in CMW-R1513P98

None

Operation changes in CMW-R1513P97

None

Operation changes in CMW-R1513P95

None

Operation changes in CMW-R1513P89

None

Operation changes in CMW-R1513P85

None

Operation changes in CMW-R1513P81

None

Operation changes in CMW-R1513P66

None

Operation changes in CMW-R1513P62

- The device temperature is no longer explicitly shown on the web interface, as the values previously reflected internal circuit temperatures that are high and could be misleading. The temperature display now only indicates whether the device is operating at a normal, high, or over-temperature conditions.

Operation changes in CMW-R1513P51

None

Operation changes in CMW-R1513P50

None

Operation changes in CMW-R1513P15

None

Operation changes in CMW-R1513P13

None

Operation changes in CMW-R1513P07

None

Operation changes in CMW-R1513P06

None

Operation changes in CMW-R1513P05

- Changed the default state of all TCP/UDP ports from "enabled" to "disabled", including TCP port 7547, and UDP port 161.

Operation changes in CMW-R1513P01

- 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 CMW-R1513

- Added a function of enabling or disabling IPv6 on the **Network** > **IPv6 Management**> **IPv6 Service** Web page for the 1910.
- If the configuration is saved on a switch where a software version of R1513 or higher is running but the software version in the startup configuration file is still lower than F1510 (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**.

Operation changes in CMW-R1512P10

None

Operation changes in CMW-R1512P05

None

Operation changes in CMW-R1511

None

Operation changes in CMW-F1510

None

Operation changes in CMW-R1112

None

Operation changes in CMW-R1111P02

None

Operation changes in CMW-R1111P01

After you downgrade a 1910 switch from Release R1111P01 or above to an earlier version than Release R1111P01, its SysOid changes to identify the switch as a 3COM 2900 device, but the change does not affect the use of the switch. For the HP 1910 and 3Com 2900 switch mapping, see "HP 1910 product family matrix."

Operation changes in CMW-R1111

None

Operation changes in CMW-R1109

1. Merge the ".xml" configuration into the ".cfg" configuration.
2. The Key can be auto-generated for the SSH service on the **Web->Network->Service** page.
3. The PKI certificate can be auto-generated for HTTPS service on the **Web->Network->Service** page.

Operation changes in CMW-R1108P01

None

Operation changes in CMW-R1108

None

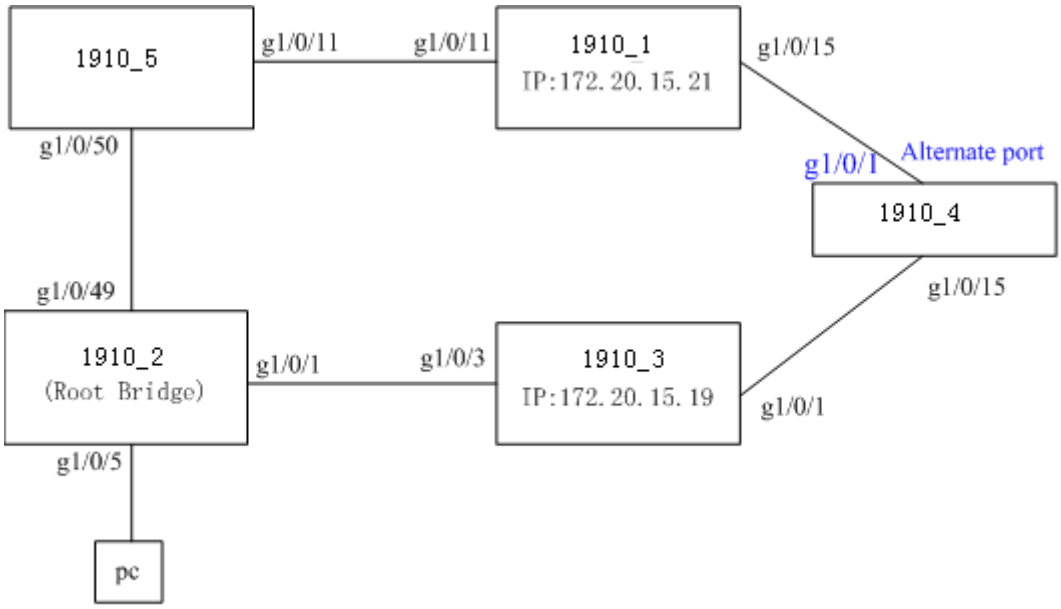
Restrictions and cautions

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

LSD44945

- Symptom: In the following network diagram, a ping operation from the PC to 1910_1 experiences a 30-second interruption.
- Condition: This symptom might occur when the following conditions exist:
  - All 1910 switches and the PC are in the same subnet.
  - MSTP is configured to avoid loops and all 1910 switches belong to MSTP instance 0.
  - The port G1/0/49 of the root bridge 1910_2 is shut down.



- Workaround: Configure the **stp no-agreement-check** command on the root ports.

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 F1510 , 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 GE copper port is connected to a device that uses a RealTek RTL8169 network chip, the port goes up and down twice, and then goes up.
- Condition: This symptom might occur when a GE copper port is connected to a device that uses a RealTek RTL8169 network chip.
- 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 R1515

201507210240

- Symptom: The switch reboots unexpectedly when the FreeRADIUS server issues a command to force an 802.1X user offline.

- Condition: This symptom might occur if the switch uses a FreeRADIUS server for 802.1X authentication.

201506180309

- Symptom: The DHCP server on the switch does not preferentially use the static address pool when processing DHCP-INFORM packets.
- Condition: This symptom might occur if the following conditions exist:
  - The DHCP-INFORM packets are sent by a DHCP client bound to an IP address in the static address pool.
  - The address range of a dynamic address pool covers the static address pool.

Resolved problems in R1513P99

201504090198

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

201504090198

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

201504090198

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

201504090198

- Symptom: CVE-2015-0289
- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201504090198

- Symptom: CVE-2015-0292
- Condition: A vulnerability existed in previous versions of OpenSSL related to the processing of base64 encoded data.

201505150250

- Symptom: A user cannot pass the RADIUS authentication.
- Condition: This symptom occurs when the attributes issued by the RADIUS server are as follows during the RADIUS authentication/authorization process:
  - The attribute 65 (Tunnel-Medium-Type) is set to 802.

- The attribute 64 (Tunnel-Type) is set to VLAN.
- No VLAN ID is configured in the attribute 81 (Tunnel-Private-Group-ID).

Resolved problems in R1513P98

201504290276

- Symptom: The **ip address dhcp-alloc client-identifier mac vlan-interface1** command in the configuration file cannot be issued correctly to a switch during its startup with factory default settings.
- Condition: This symptom occurs if the switch has the **ip address dhcp-alloc** command enabled by default on interface Vlan-interface 1.

201504280034

- Symptom: The unsupported command **cwmp cpe inform interval enable** appears in the configuration file after the switch restarts.
- Condition: This symptom occurs if the ACS has issued CMWP parameters to the switch during its startup with factory default settings.

201504200154

- Symptom: After being logged out, an authenticated user can access Internet resources without passing portal authentication in triple authentication.
- Condition: This symptom occurs if the cable is removed from and then installed into the interface connected to the user after the user passes the previous portal authentication.

201504200154

- Symptom: MAC authentication succeeds after a delay of 20 to 30 seconds.
- Condition: This symptom occurs if both portal authentication and MAC authentication are configured for triple authentication.

201502270197

- Symptom: iMC is disconnected from a managed switch and generates an ICMP no response alarm for the switch.
- Condition: This symptom occurs if the switch suffers from attacks against the ipForwarding and ipDefaultTTL nodes.

Resolved problems in R1513P97

201503110433

- Symptom: The PVST topology changes after the device runs at 100% CPU usage for a period.
- Condition: This symptom can be seen when the **display interface** command is repeatedly executed.

201501210266

- Symptom: CVE-2015-0205
- Condition: An OpenSSL server will accept a DH certificate for client authentication without the certificate verify message. This effectively allows a client to authenticate without the use of a private

key. This only affects servers which trust a client certificate authority which issues certificates containing DH keys.

201501210266

- Symptom: CVE-2014-3570
- Condition: Bignum squaring (BN_sqr) may produce incorrect results on some platforms, including x86_64. This bug occurs at random with a very low probability, and is not known to be exploitable in any way.
- 201501210266
- Symptom: CVE-2015-0204
- Condition: An OpenSSL client will accept the use of an RSA temporary key in a non-export RSA key exchange ciphersuite. A server could present a weak temporary key and downgrade the security of the session.

201501210266

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

201501210266

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

201501210266

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

Resolved problems in R1513P95

201412310369

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

201410230226

- Symptom: SSL 3.0 Fallback protection
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to

SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

201410130567

- Symptom: IP broadcast packets cannot be relayed and forwarded.
- Condition: This symptom occurs when the **udp-helper server** command is executed on a Layer 3 virtual interface to configure the IP address of the destination server for UDP helper as a subnet broadcast address.

201407040459

- Symptom: SPI conflicts occur during IKE SA establishment.
- Condition: This symptom can be seen when the switch uses IKE autonegotiation to establish SAs with the peer.

201407040368

- Symptom: A software upgrade through IMC BIMS fails.
- Condition: This symptom can be seen if you use IMC BIMS to upgrade software.

201405080424

- Symptom: DHCP clients cannot obtain IP addresses through a DHCP relay agent.
- Condition: This symptom can be seen if the DHCP relay agent fails to forward DHCP packets from DHCP clients for reasons such as connectivity issues.

201404040393

- Symptom: A user fails to log in to the switch.
- Condition: This symptom occurs if the following conditions exist:
  - The user uses RADIUS authentication.
  - The RADIUS server assigns multiple login-service attributes for the user.

201404040371

- Symptom: The switches in an IRF fabric cannot learn the MAC addresses of some attached servers.
- Condition: This symptom can be seen after a new member switch is added to the IRF fabric.

201404040238

- Symptom: A DHCP client takes a long time to request an IP address.
- Condition: This symptom occurs when the VLAN interface enabled with the DHCP server is not on the same subnet as the IP address requested by the DHCP client. The DHCP server does not respond with a NAK packet, so the client sends the request multiple times before sending a Discovery packet.

201404040141

- Symptom: The switch unexpectedly reboots when the DHCP server receives a DHCP request.
- Condition: This symptom occurs if the DHCP request contains Option 82 sub-option 5 that is longer than four bytes.

201501080315

- Symptom: When you display information about the transceiver module of an interface, the output shows that the connector type is UNKNOWN.

- Condition: This symptom occurs when the interface has Finisar 1000_BASE_T_AN_SFP transceiver module installed.

201412180325

- Symptom: DHCP clients are not assigned the options parameters configured in a DHCP server address pool.
- Condition: This symptom can be seen if the DHCP requests sent by DHCP clients do not include requested parameters in Option 55.

201411060566

- Symptom: Some files in the nand flash of the switch are lost.
- Condition: This symptom can be seen when errors exist in the nand flash of the switch.

Resolved problems in R1513P89

201409110254

- Symptom: The nonstandard PD detection setting cannot survive a switch reboot.
- Condition: This symptom occurs when the setting is successfully saved after nonstandard PD detection (the **poe legacy enable** command) is enabled on the Web page.

201409020106

- Symptom: CVE-2008-5161
- Description: Error handling in the SSH protocol in several SSH servers/clients, including OpenSSH 4.7p1 and possibly other versions, when using Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data.

201408220454

- Symptom: CVE-2014-3508
- Condition: A flaw in OBJ_obj2txt may cause pretty printing functions such as X509_name_oneline, X509_name_print_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

201406120024

- Symptom: CVE-2014-0224.
- Condition: When Open SSL Server or Client is used.

Resolved problems in CMW520-R1513P85

201403190486

- Symptom: A PoE-capable switch cannot provide power to NJ2000.
- Condition: This symptom can be seen after the software is upgraded from R1112 to R1513P81.

201401230151

- Symptom: The device panel on the Web page displays incorrect port state information.
- Condition: This symptom can be seen after the device panel Web page has been refreshing for more than two hours through Internet Explorer.

Resolved problems in CMW520-R1513P81

201311130592

- Symptom: During an HTTPS login by Google Chrome browser with version 27.0.1453.116, memory leaks occur, and system memory is exhausted.
- Condition: This symptom occurs when the following conditions exist:
  - The **ip https enable** command is configured on the switch.
  - No password is configured for HTTPS login.

201310310126

- Symptom: A unicast ARP packet received on an interface is forwarded by that interface.
- Condition: This symptom occurs when the following conditions exist:
  - The interface is a member interface of an aggregation group.
  - The egress interface of the MAC entry that matches the destination MAC address of the unicast ARP packet is the aggregate interface corresponding to the aggregation group.

201308300174

- Symptom: The switch fails to convey the user priority assigned by the RADIUS server to a user.
- Condition: This symptom occurs when RADIUS scheme-based SSH authentication is used.

Resolved problems in CMW520-R1513P66

None

Resolved problems in CMW520-R1513P62

201308200031

- Symptom: If a domain name configured in the Web interface has more than 25 characters, only the first 25 characters take effect.
- Condition: This symptom can be seen if a domain name configured in the Web interface has more than 25 characters.

201308210419

- Symptom: Using the **password** command to modify the password of a user gets a prompt that the username is correct.
- Condition: This symptom occurs if the user is created in the Web interface and irreversible password encryption is used.

Resolved problems in CMW520-R1513P51

LSD075204

- Symptom: If IE10 is used to access the Web interface of the switch, some Web pages fail to work. For example, the **Cancel** button on the **PoE>Port Setup** page does not work.

- Condition: This symptom occurs if IE10 is used to access the Web interface of the switch.

LSD075320

- Symptom: When an ARP detection trusted port is attacked by large numbers of ARP packets, the users connected to the switch might lose connection.
- Condition: This symptom might occur when an ARP detection trusted port is attacked by large numbers of ARP packets.

Resolved problems in CMW520-R1513P50

LSD075026

- Symptom: Using the IE10 browser to access the Web interface of the switch fails.
- Condition: This symptom occurs because the Web interface does not support IE10.

LSD075114

- Symptom: After a cable that connects a PoE port to a Sony DV is removed and inserted, the DV does not work.
- Condition: This symptom occurs after a cable that connects a PoE port to a Sony DV is removed and inserted.

LSD074731

- Symptom: Failed to upload files to an appointed path when authentication is required by iMC BIMs.
- Condition: When system try to upload a file to iMC BIMs and authentication is required.

Resolved problems in CMW520-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 contiguous.

Resolved problems in CMW520-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.

LSD074123

- Symptom: The switch fails to upgrade the PoE firmware.

- Condition: This symptom occurs during a PoE firmware upgrade.

Resolved problems in CMW520-R1513P07

LSD073500

- Symptom: When a PC connected to a 1910 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 a 1910 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.

LSD073921

- Symptom: Users' STACK function cannot be used.
- Condition: This symptom occurs because NTDP&NDP is disabled on the switch by default.

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 CMW520-R1513P06

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.

LSD073066

- Symptom: The NTP Web page displays garbage characters.
- Condition: This symptom might occur if you modify and save NTP settings when the switch runs a version between R1109 and R1513P05, and then upgrade the software to R1513P05.

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 CMW520-R1513P05

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.

LSD072681

- Symptom: After the software is upgraded to R1109 or higher, the settings configured in the old version on the web idle timeout, syslog buffer, ntp server1, ntp server2 Web pages do not take effect.
- Condition: This symptom occurs if all or parts of these settings have been configured before the software is upgraded to R1109 or higher.

LSD072813

- Symptom: An IRF member device reboots unexpectedly when STP topology flapping occurs repeatedly.
- Condition: This symptom occurs if the following conditions exist:
  - STP topology flapping occurs repeatedly
  - The numbers of DHCP address pools and MAC address entries reach the upper limits on the device.

Resolved problems in CMW520-R1513P01

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 CMW520-R1513

LSD072305

- Symptom: IPv6 cannot be enabled in the Web interface after the software is upgraded from a version lower than F1510 to F1510 or higher.
- Condition: This symptom occurs after the software is upgraded from a version lower than F1510 to F1510 or higher.

LSD071416

- Symptom: Some Web pages for 1910, such as ACL IPv6, IPv6 router, and IPv6 ping/traceroute pages, do not provide online help information.
- Condition: This problem exists on some Web pages for 1910.

Resolved problems in CMW520-R1512P10

LSD072006

- Symptom: The IPv6 does not work.
- Condition: This symptom might occur after the switch is upgraded from a version earlier than F1510 to F1510 or later.

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 CMW520-R1512P05

LSD071395

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

Resolved problems in CMW520-R1511

None

Resolved problems in CMW520-F1510

ZDD05100

- Symptom: The switch updates ARP entries for only 32 MAC addresses when a large number of MAC addresses are moved to different ports.
- Condition: This symptom might occur when a large number of MAC addresses are moved to different ports.

Resolved problems in CMW520-R1112

ZDD05003

- Symptom: The CLI does not respond.

- Condition: This symptom might occur when the switch is accessed through SNMPv3 using 3DES authentication.

ZDD04990

- Symptom: The switch might automatically close the HTTPS service (TCP port 443), and the web interface of the switch cannot be accessed through HTTPS (or SSH login fails).
- Condition: This symptom might occur if the following conditions exist:
  - HTTPS is enabled on the switch.
  - Use HTTPS to access the web interface of the switch.

ZDD04944

- Symptom: The switch reboots when it requests an IP address from a DHCP server.
- Condition: This symptom might occur if the following conditions exist:
  - The DHCP server assigns multiple DHCP options.
  - DHCP client debugging is enabled on the switch..

ZDD04931

- Symptom: The switch enabled with the DHCP server reboots when a PC accesses it through Web.
- Condition: This symptom might occur if the following conditions exist:
  - DHCP option 3 or 6 is configured as a string of 255 ASCII characters on the DHCP server.
  - A PC accesses the DHCP server through Web.

ZDD04865

- Symptom: The switch reboots when an SSH user logs in.
- Condition: This symptom might occur if the free memory space of the switch is insufficient.

ZDD04706

- Symptom: RADIUS authentication fails when the Vendor-Specific attribute sent by the RADIUS server is not in the standard TLV format.
- Condition: This symptom might occur when the Vendor-Specific attribute sent by the RADIUS server is not in the standard TLV format.

LSD69613

- Symptom: The device information on the **Summary > Device Information** web page does not show port states.
- Condition: None.

LSD69165

- Symptom: The GMT offset for Caracas is wrong on the **Device > System Time** time zone web page .
- Condition: None.

LSD47115

- Symptom: An error message might appear during an operation on the **PoE > PoE >Port Setup** web page.
- Condition: None.

Resolved problems in CMW520-R1111P02

LSD071600

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

Resolved problems in CMW520-R1111P01

None

Resolved problems in CMW520-R1111

LSD65011

- Symptom: Garbled characters appear on the **Network > LLDP > Neighbor Summary** web page.
- Condition: This symptom exists in the **Network > LLDP > Neighbor Summary** Web page.

LSD64981

- Symptom: A newly configured gateway might not overwrite the previous one when the gateway is configured multiple times through the **Wizard** web page.
- Condition: This symptom might occur when the gateway is configured multiple times through the **Wizard** web page.

LSD47162

- Symptom: IMC might not display an error message when QoS application on IMC fails.
- Condition: This symptom might occur when QoS application on IMC fails.

LSD50868

- Symptom: The **Network > IGMP Snooping** Web page is not easy to use due to lack of operation help information.
- Condition: This symptom exists in the **Network > IGMP Snooping** Web page.

LSD50752

- Symptom: 10K-long packets cannot be forwarded between two ports on a V1910-48G switch.
- Condition: This symptom might occur when the port number of one port is between 1 and 24 and that of the other is between 25 and 48.

LSD64667

- Symptom: The CLI of the switch might not respond after an NMS running SNMPTest connects to the switch as an SNMPv3 user using the SHA-3DES encryption algorithm.
- Condition: This symptom might occur when the SNMPv3 user account uses the SHA-3DES encryption algorithm and the NMS runs SNMPTest to connect to the switch.

ZDD04517

- Symptom: A DISMAN-PING-MIB::pingResultsOperStatus access failure occurs and the switch cannot recover from the failure and reboots occasionally.
- Condition: This symptom might occur when NQA operations continuously and quickly get or set the RPINGMib.

ZDD04543

- Symptom: The switch running LLDP reboots when the **display lldp neighbor-information** command is executed.
- Condition: This symptom might occur if the **display lldp neighbor-information** command is executed after the switch receives an LLDP packet in which the LCI length in the location ID TLV is 0.

ZDD04556

- Symptom: The switch running LLDP reboots when the **display lldp neighbor-information** command is executed.
- Condition: This symptom might occur if the **display lldp neighbor-information** command is executed after the switch receives an LLDP packet that has an organization-unknown TLV larger than 500 bytes.

ZDD04569

- Symptom: The switch reboots when receiving large amounts of traffic.
- Condition: This symptom might occur when the **debugging vty negotiate** command is enabled.

ZDD04596

- Symptom: The switch might reboot when it has large amounts of FTP traffic to process.
- Condition: None.

LSD67635

- Symptom: Walking MIB node entPhysicalHardwareRev.15 returns an incorrect value.
- Condition: This symptom might occur during a walk on MIB node entPhysicalHardwareRev.15.

Resolved problems in CMW520-R1109

LSD63498

- Symptom: The gateway IP address could not be set in the web wizard.
- Condition: This symptom exists in the Web wizard.

LSD63499

- Symptom: The SSH service and HTTPS service are automatically enabled when the switch starts up (see the **Web > Network > Service** page), making key or PKI certificate key unable to be generated automatically.
- Condition: None.

LSD61667

- Symptom: The file list on the web page might contain an ".XML" file.
- Condition: None.

ZDD04165

- Symptom: The value of the Chassis ID field in the LLDP log information is garbled characters.
- Condition: This symptom might occur when the switch is connected to a Cisco IP phone and LLDP is enabled.

ZDD04178

- Symptom: The source MAC-based ARP attack detection function could not detect and protect the switch against ARP attacks from fixed MAC addresses. And might affect the normal ARP learning function.
- Condition: This symptom might occur when the attack sources reside on a different network segment than the interface.

ZDD04254

- Symptom: The FTP data session could not be established.
- Condition: This symptom might occur when the switch is used as the FTP client and the prompt of the FTP server is not that given in the RFC document.

Resolved problems in CMW520-R1108P01

LSD63812

- Symptom: The SFP ports are always down at the Link layer or the port statistics show the number of erroneous input packets constantly increase.
- Condition: This symptom might occur when the settings for the speed and duplex working mode parameters are both auto-negotiation.

Resolved problems in CMW520-R1108

- This is the first release version.

Related documentation

Documentation set

- *Read This First (5998-1520)*
- *HP Small Biz Feedback (5998-2984)*
- *HP 1910-8G Switch Series Compliance and Safety Manual*
- *HP 1910 Gigabit Ethernet Switch Series Compliance and Safety Manual*
- *HP 1910 Gigabit Ethernet Switch Series Getting Started Guide*
- *HP 1910 Gigabit Ethernet Switch Series User Guide-Release 1513*

Obtaining documentation

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

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

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

Table 5 1910 series hardware features

Item	Description
Physical dimensions (H × W × D)	43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (1910-16G) 43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in.) (1910-24G) 43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in.) (1910-48G) 43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in.) (1910-24G-PoE (170W)) 43.6 × 440 × 420 mm (1.72 × 17.32 × 16.54 in.) (1910-24G-PoE (365W)) 43.6 × 210 × 210 mm (1.72 × 8.27 × 8.27 in.) (1910-8G) 43.6 × 300 × 260 mm (1.72 × 11.81× 10.24 in.) (1910-8G-PoE+ (65W) 43.6 × 300 × 260 mm (1.72 × 11.81× 10.24 in.) (1910-8G-PoE+ (180W))
Weight	≤ 3 kg (6.61 lb) (1910-16G) ≤ 3 kg (6.61 lb) (1910-24G) ≤ 5 kg (11.02 lb) (1910-48G) ≤ 6 kg (13.22 lb) (1910-24G-PoE (170W)) ≤ 7 kg (15.43 lb) (1910-24G-PoE (365W)) ≤ 2 kg (4.406 lb) (1910-8G) ≤ 3 kg (6.61 lb) (1910-8G-PoE+ (65W)) ≤ 3 kg (6.01 lb) ((1910-8G-PoE+ (180W))
Console port	1
Service ports	16 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (1910-16G) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (1910-24G) 48 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (1910-48G) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (1910-24G-PoE (170W)) 24 × 10/100/1000Base-T autosensing Ethernet ports + 4 GE SFP interfaces (1910-24G-PoE (365W)) 8 × 10/100/1000Base-T autosensing Ethernet ports + 1 GE SFP interfaces (1910-8G) 8 × 10/100/1000Base-T autosensing Ethernet ports + 1 GE SFP interfaces (1910-8G-PoE+ (65W)) 8 × 10/100/1000Base-T autosensing Ethernet ports + 1 GE SFP interfaces (1910-8G-PoE+ (180W))

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 1910-24G-PoE (365W) supports RPS DC input
Power consumption (full configuration)	25.1 W (1910-16G) 31.5 W (1910-24G) 59.8 W (1910-48G) 255 W (85 W for system power consumption and 170 W for PoE power consumption) (1910-24G-PoE (170W)) AC power input: 528 W (158 W for system power consumption and 370 W for PoE power consumption) (1910-24G-PoE (365W)) DC power input: 832 W (92 W for system power consumption and 740 W for PoE power consumption)) (1910-24G-PoE (365W)) 14.4 W (1910-8G) 95W (1910-8G-PoE+ (65W)) 230W (1910-8G-PoE+ (180W))
Operating temperature	0°C to 45°C (32°F to 113°F)
Operating humidity (noncondensing)	10% to 90%

Software features

Table 6 Software features of the V1910 series

Category	Features
Link aggregation	Dynamic aggregation of Gigabit Ethernet (GE) ports Dynamic link aggregation through Link Aggregation Control Protocol (LACP) Manual link aggregation Supports up to (total number of ports/2) link aggregation groups, each supporting up to eight GEs
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 Blackhole MAC addresses MAC address learning limit on a port

Category	Features
VLAN	Port-based VLANs (256 VLANs) Voice VLAN
ARP	256 entries 64 static entries
VLAN virtual interface	8
IP Unicast route	Support IPv4 / IPv6 static route
Multicast	IGMP Snooping MLD Snooping
DHCP	DHCP client DHCP snooping DHCP relay agent
Broadcast/multicast/unicast storm control	Storm control based on port rate percentage PPS-based storm control bps-based storm control
MSTP	STP/RSTP/MSTP protocol Up to four spanning tree instances STP root protection BPDU protection
QoS/ACL	802.1p/DSCP precedence marking Four queues per port SP, WRR, and SP+WRR queue scheduling algorithms Port-based rate limit, with a minimum granularity of 64-kbps Flow-based traffic redirecting Time ranges Support IPv6 ACL
Mirroring	Port mirroring
Security features	Hierarchical management and password protection of users AAA authentication RADIUS authentication Port isolation 802.1X Portal
802.1X	Up to 1024 users Port-based and MAC address–based authentication Guest VLAN
Loading and upgrade	Loading and upgrade through XModem protocol Loading and upgrade through trivial file transfer protocol (TFTP)
Management	Simple Network Management Protocol (SNMP) Remote Monitoring (RMON) alarm, event and history recording

Category	Features
	DM NMS
	Web NMS
	System log
	Hierarchical alarms
	Stacking management
	NTP
	Power, fan, and temperature alarms
	pingv6
	tracertv6
Maintenance	Debugging information output
	ping and tracert
	Virtual cable test

Appendix B Upgrading software

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

Table 7 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	Upgrading at the CLI

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 1910-8G-PoE+ (65W) Switch BOOTROM, Version 171             *
*                                                                            *
******************************************************************************
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.

Creation Date       : Dec 21 2012
CPU L1 Cache        : 32KB
CPU Clock Speed     : 333MHz
Memory Size         : 128MB
Flash Size          : 128MB
CPLD Version        : 001
PCB Version         : Ver.A
Mac Address         : 000EFB000020

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

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

Table 8 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 171                       *
*                                                                           *
*****************************************************************************

   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 9 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 10 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 11).

   ```
   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 11 Extended Boot ROM menu options

Option	Tasks
1. Download application file to flash	Download a .bin software package file to the flash. If password recovery capability is enabled, you can use any version of the system software image for upgrade. If password recovery capability is disabled, you can use only the Release 1513P07 version (or higher) for upgrade.
2. Select application file to boot	Specify the main and backup system software images for the next startup: • 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	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.

Option	Tasks
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 12.

Table 12 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.

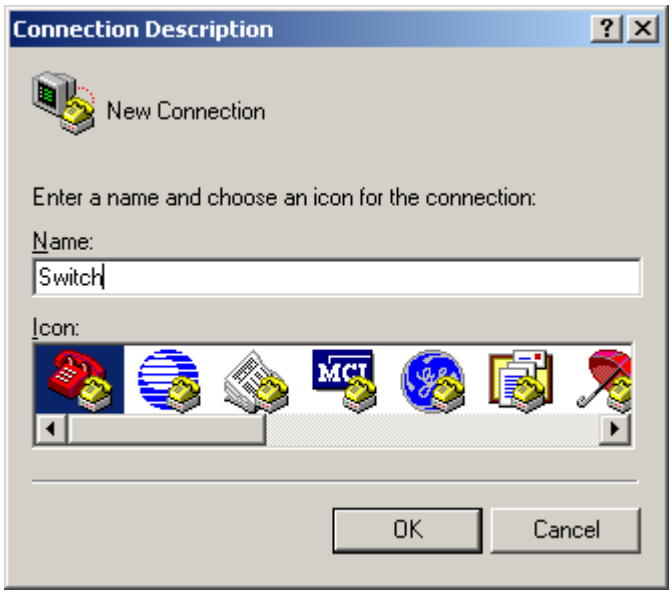
The following are the required terminal settings:

- Bits per second—38,400
- 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:

Step1 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

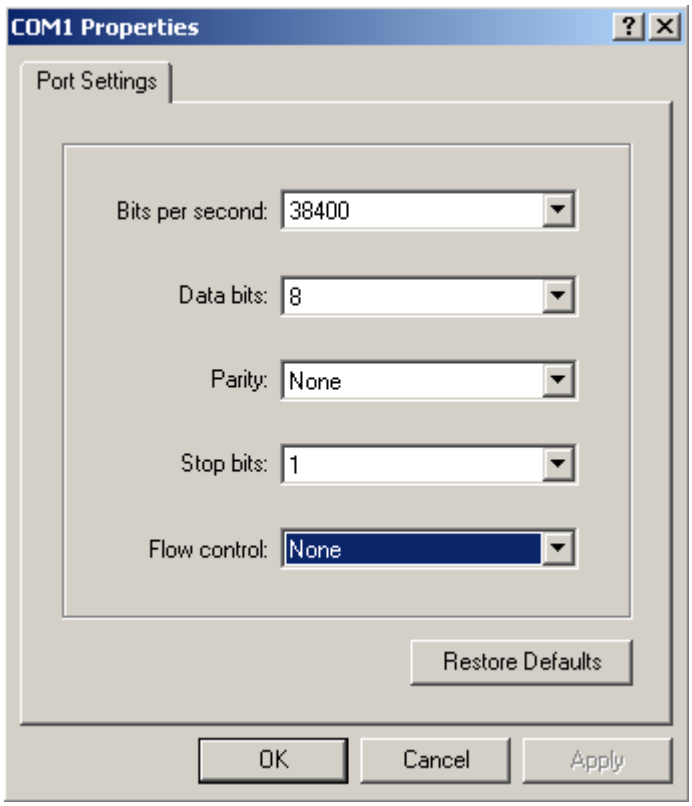


Step2 Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

Figure 2 Set the serial port used by the HyperTerminal connection

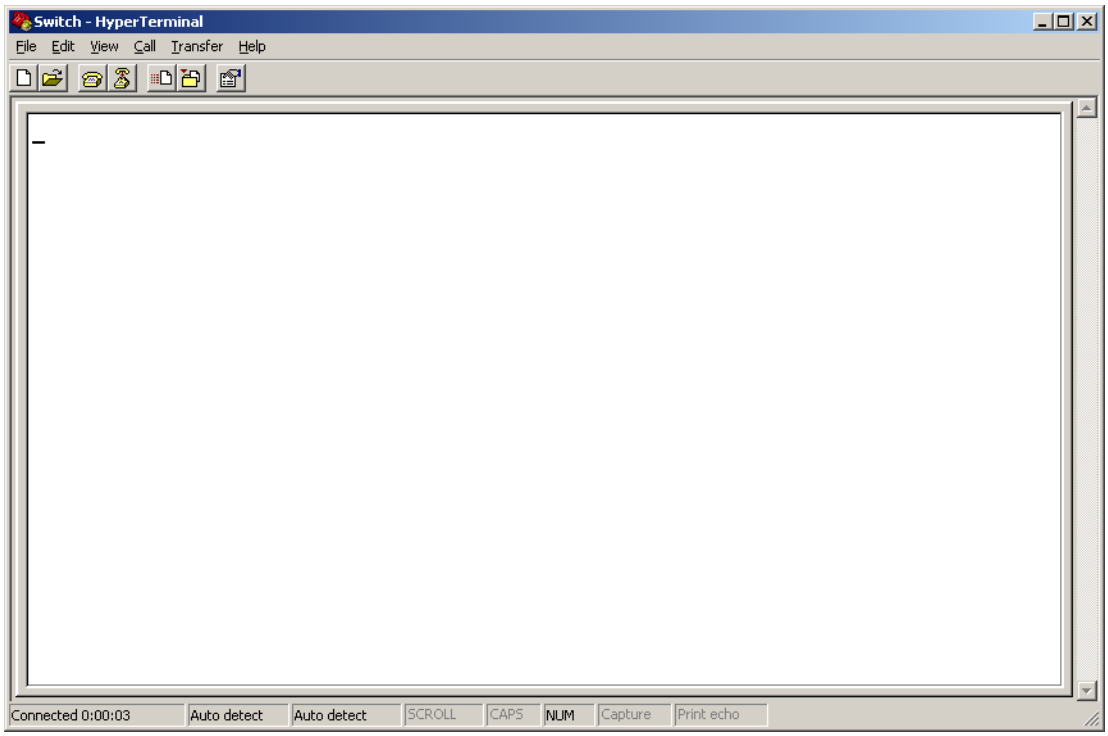
Step3 Set **Bits per second** to **38400**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

Figure 3 Set the serial port parameters



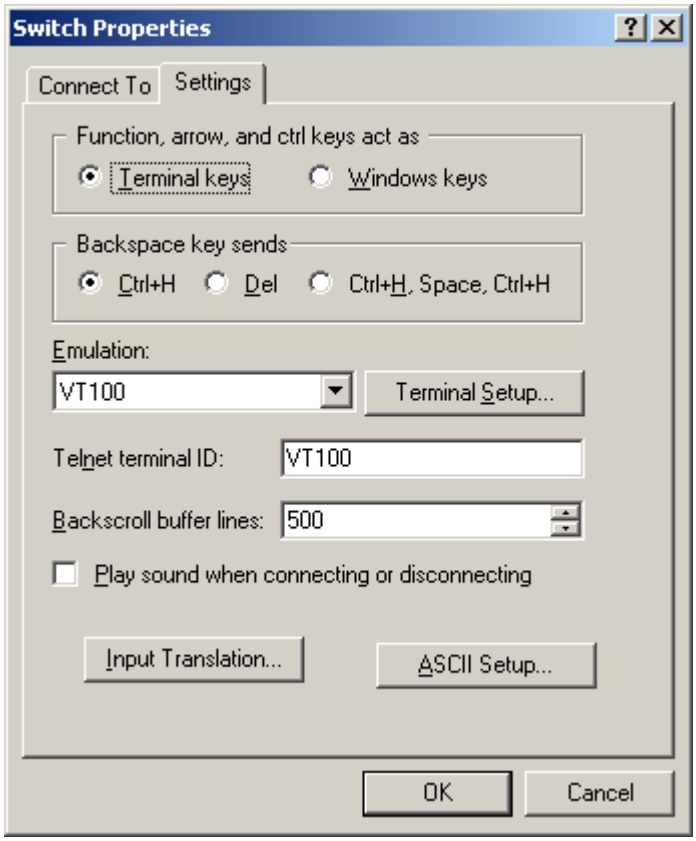
Step4 Select **File** > **Properties** in the HyperTerminal window.

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):
```

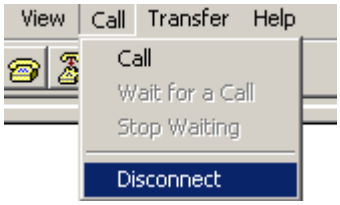
4. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
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 38400 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

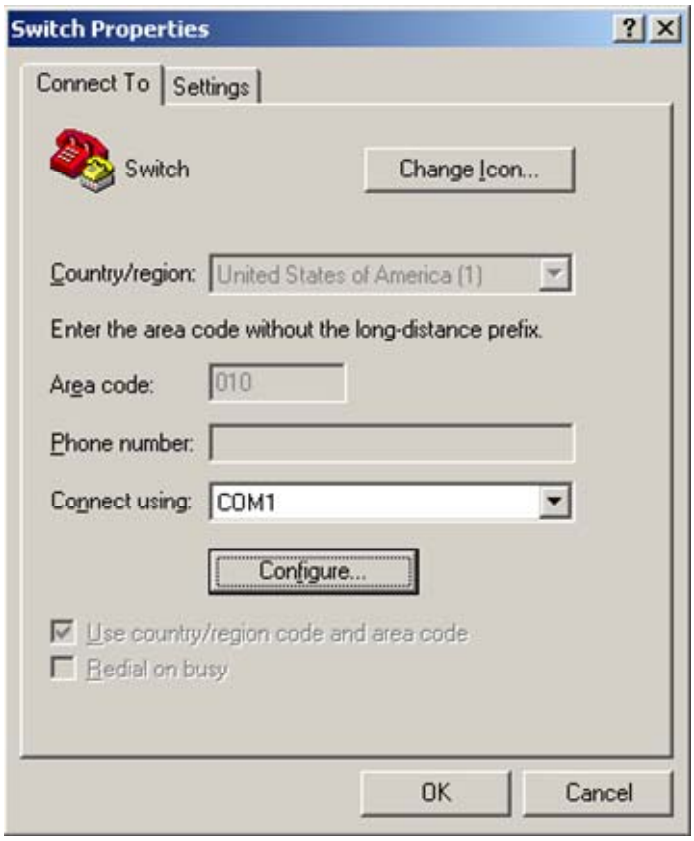
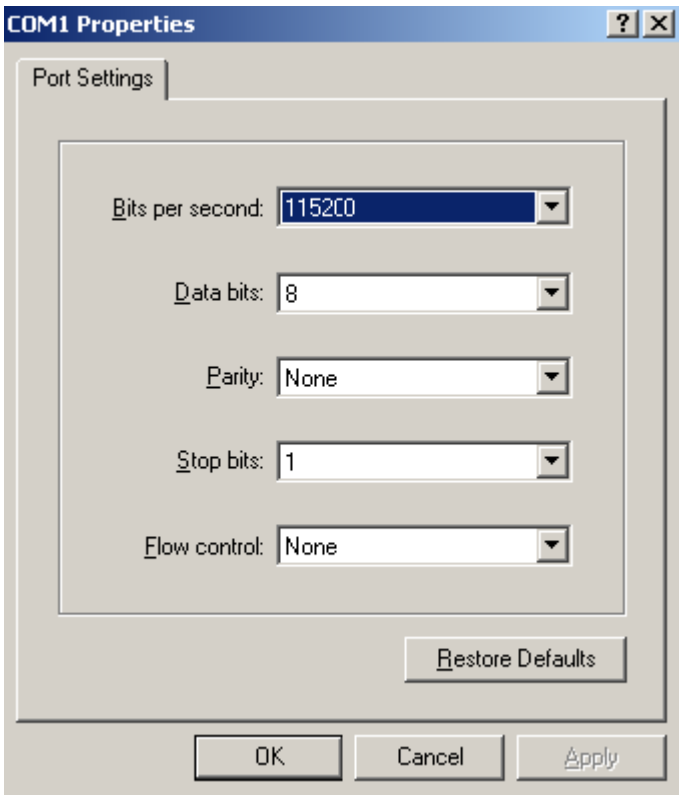
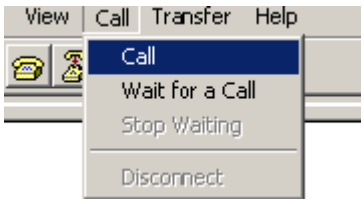


Figure 8 Modify the baud rate



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

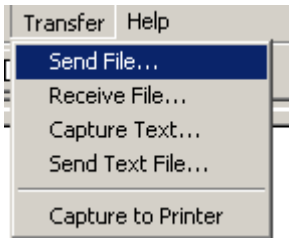
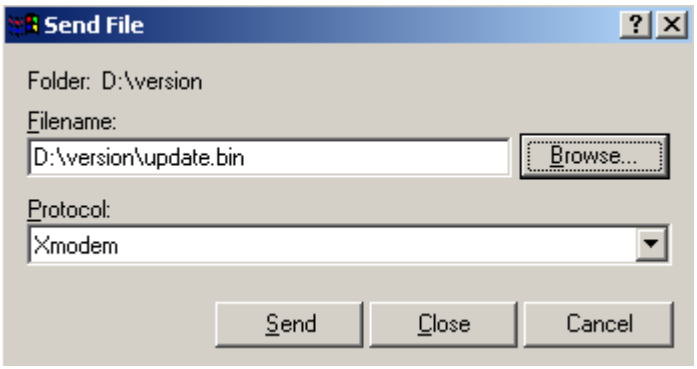
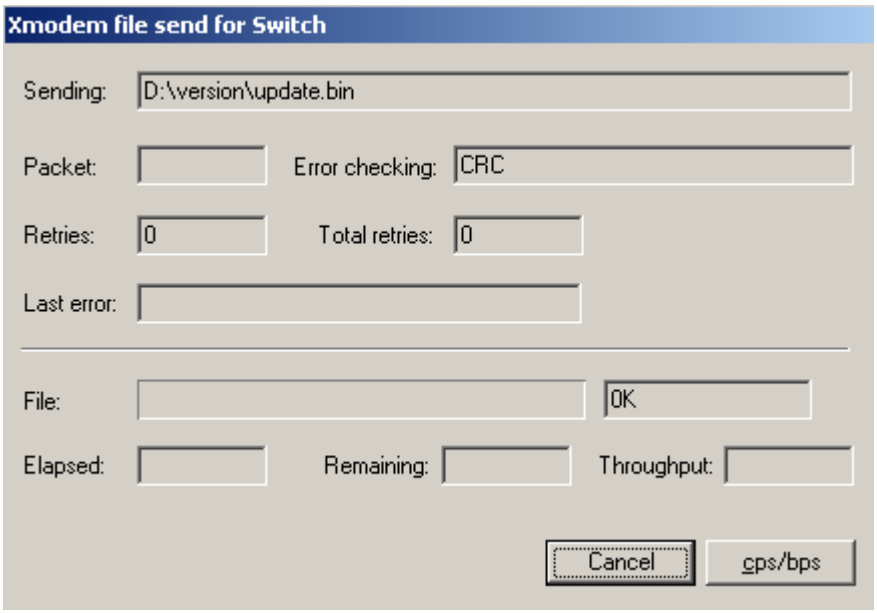


Figure 11 File transmission dialog box



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 38400 bps, press ENTER when ready.
```

8. If you are using a download rate other than 38400 bps, restore the baud rate of the serial port on the terminal to 38400 bps. If the baud rate is 38400 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 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):
```

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 of the switch to the server and connect the console port of the switch to a PC

NOTE:

- The PC and the TFTP/FTP server can be co-located.
- The HP V1910 Switche Series 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 13 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):
```

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 of the switch to the server and connect the console port of the switch to a PC.
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       :V1910
FTP User Password   :V1910
```

Table 14 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)

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)
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):
```

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

Loading Software Using TFTP

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

Step 1: Configure an IP address for the switch

```
<HP V1910 Switch>ipsetup ip-address 192.168.1.2 24
```

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

```
<HP V1910 Switch>upgrade 192.168.1.1 update.bin runtime
The file flash:/ main.bin exists. Overwrite it? [Y/N]:y
  Verifying server file...
  Deleting the old file, please wait...

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait.../
  TFTP: 10262272 bytes received in 104 second(s)
  File downloaded successfully.

  The specified file will be used as the boot file at the next reboot.
```

Step 3: Download and load the Boot ROM file.

```
<HP V1910 Switch>upgrade 192.168.1.1 update.btm bootrom

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP:   259324 bytes received in 2 second(s)
  File downloaded successfully.
   BootRom file updating finished!
```

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

```
<HP V1910 Switch> reboot
```

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