Hewlett Packard
Enterprise

HPE OfficeConnect 1920 Switch Series CMW520-R1120 Release Notes

Contents

Version information ··· 1

Version number ··· 1

Version history ··· 1

Hardware and software compatibility matrix ··· 9

Upgrading restrictions and guidelines ··· 10

Hardware feature updates ··· 10

Software feature and command updates ··· 10

MIB updates ··· 11

Operation changes ··· 12

Restrictions and cautions ··· 12

Open problems and workarounds ··· 14

List of resolved problems ··· 14

Resolved problems in CMW520-R1121 ··· 14

Resolved problems in CMW520-R1120 ··· 15

Resolved problems in CMW520-R1119 ··· 15

Resolved problems in CMW520-R1118 ··· 15

Resolved problems in CMW520-R1117 ··· 15

Resolved problems in CMW520-R1116 ··· 15

Resolved problems in CMW520-R1115 ··· 16

Resolved problems in CMW520-R1114 ··· 16

Resolved problems in CMW520-R1113 ··· 18

Resolved problems in CMW520-R1112 ··· 18

Resolved problems in CMW520-R1111 ··· 18

Resolved problems in CMW520-R1110 ··· 18

Resolved problems in CMW520-R1109 ··· 18

Resolved problems in CMW520-R1108 ··· 19

Resolved problems in CMW520-R1107 ··· 20

Resolved problems in CMW520-R1106 ··· 21

Resolved problems in CMW520-R1105 ··· 21

Resolved problems in CMW520-R1104 ··· 21

Resolved problems in CMW520-R1103 ··· 21

Resolved problems in CMW520-R1102 ··· 22

Support and other resources ··· 22

Accessing Hewlett Packard Enterprise Support ··· 22

Documents ··· 22

Related documents 22
Documentation feedback 22
Appendix A Feature list 24
Hardware features 24
Software features 26
Appendix B Upgrading software 28
System software file types 28
Upgrade methods 28
Preparing for the upgrade 28
Upgrading from the WEB 29
Upgrading from the BootWare menu 30
Accessing the BootWare menu 30
Using TFTP/FTP to upgrade software through an Ethernet port 32
Using XMODEM to upgrade software through the console port 33
Managing files from the BootWare menu 38
Displaying all files 39
Changing the type of a system software image 39
Deleting files 40
Handling software upgrade failures 40

List of Tables

Table 1 Version history 1

Table 2 Hardware and software compatibility matrix 9

Table 3 MIB updates 11

Table 4 Table-Max hardware forwarding table resources for forwarding 13

Table 5 HPE OfficeConnect 1920 Switch Series hardware features 24

Table 6 Software features of the HPE OfficeConnect 1920 Switch Series 26

Table 7 BootWare menu options 31

Table 8 Ethernet submenu options 32

Table 9 Network parameter fields and shortcut keys 32

Table 10 Serial submenu options 34

Table 11 File Control submenu options 39

This document describes the features, restrictions and guidelines, open problems, and workarounds for version CMW520-R1121. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with HPE 1920-CMW520-R1121 Release Notes (Software Feature Changes) and the documents listed in "Related documents"

Version information

Version number

Comware Software, Version 5.20.99, Release 1121

You can see the version information by using the **summary** command in any view. See **Note 1**.

Version history

IMPORTANT:

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

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
JG920A-CMW520-R1121	JG920A-CMW520-R1120	2019-1-28	Release version	This version fixed bugs
JG921A-CMW520-R1121	JG921A-CMW520-R1120			
JG922A-CMW520-R1121	JG922A-CMW520-R1120			
JG923A-CMW520-R1121	JG923A-CMW520-R1120			
JG924A-CMW520-R1121	JG924A-CMW520-R1120			
JG925A-CMW520-R1121	JG925A-CMW520-R1120			
JG926A-CMW520-R1121	JG926A-CMW520-R1120			
JG927A-CMW520-R1121	JG927A-CMW520-R1120			
JG928A-CMW520-R1121	JG928A-CMW520-R1120			
JG920A-CMW520-R1120	JG920A-CMW520-R1119	2018-5-14	Release version	This version fixed bugs.
JG921A-CMW520-R1120	JG921A-CMW520-R1119			
JG922A-CMW52	JG922A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1120	R1119			
JG923A-CMW520-R1120	JG923A-CMW520-R1119			
JG924A-CMW520-R1120	JG924A-CMW520-R1119			
JG925A-CMW520-R1120	JG925A-CMW520-R1119			
JG926A-CMW520-R1120	JG926A-CMW520-R1119			
JG927A-CMW520-R1120	JG927A-CMW520-R1119			
JG928A-CMW520-R1120	JG928A-CMW520-R1119			
JG920A-CMW520-R1119	JG920A-CMW520-R1118	2017-11-21	Release version	This version fixed bugs and introduced feature changes. Modified features include: Configuring the Port ID Subtype field in the Port ID TLV through the Web interface.
JG921A-CMW520-R1119	JG921A-CMW520-R1118			
JG922A-CMW520-R1119	JG922A-CMW520-R1118			
JG923A-CMW520-R1119	JG923A-CMW520-R1118			
JG924A-CMW520-R1119	JG924A-CMW520-R1118			
JG925A-CMW520-R1119	JG925A-CMW520-R1118			
JG926A-CMW520-R1119	JG926A-CMW520-R1118			
JG927A-CMW520-R1119	JG927A-CMW520-R1118			
JG928A-CMW520-R1119	JG928A-CMW520-R1118			
JG920A-CMW520-R1118	JG920A-CMW520-R1117	2017-09-15	Release version	This version fixed bugs.
JG921A-CMW520-R1118	JG921A-CMW520-R1117			
JG922A-CMW520-R1118	JG922A-CMW520-R1117			
JG923A-CMW520-R1118	JG923A-CMW520-R1117			
JG924A-CMW520-R1118	JG924A-CMW520-R1117			
JG925A-CMW520-R1118	JG925A-CMW520-R1117			
JG926A-CMW520-R1118	JG926A-CMW520-R1117			
JG927A-CMW52	JG927A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1118	R1117			
JG928A-CMW520-R1118	JG928A-CMW520-R1117			
JG920A-CMW520-R1117	JG920A-CMW520-R1116	2017-06-27	Release version	Fixed bugs.
JG921A-CMW520-R1117	JG921A-CMW520-R1116			
JG922A-CMW520-R1117	JG922A-CMW520-R1116			
JG923A-CMW520-R1117	JG923A-CMW520-R1116			
JG924A-CMW520-R1117	JG924A-CMW520-R1116			
JG925A-CMW520-R1117	JG925A-CMW520-R1116			
JG926A-CMW520-R1117	JG926A-CMW520-R1116			
JG927A-CMW520-R1117	JG927A-CMW520-R1116			
JG928A-CMW520-R1117	JG928A-CMW520-R1116			
JG920A-CMW520-R1116	JG920A-CMW520-R1115	2017-03-28	Release version	This version fixed bugs and introduced feature changes. Modified features include: Configuring daylight saving time from the Web interface.
JG921A-CMW520-R1116	JG921A-CMW520-R1115			
JG922A-CMW520-R1116	JG922A-CMW520-R1115			
JG923A-CMW520-R1116	JG923A-CMW520-R1115			
JG924A-CMW520-R1116	JG924A-CMW520-R1115			
JG925A-CMW520-R1116	JG925A-CMW520-R1115			
JG926A-CMW520-R1116	JG926A-CMW520-R1115			
JG927A-CMW520-R1116	JG927A-CMW520-R1115			
JG928A-CMW520-R1116	JG928A-CMW520-R1115			
JG920A-CMW520-R1115	JG920A-CMW520-R1114	2016-11-25	Release version	None
JG921A-CMW520-R1115	JG921A-CMW520-R1114			
JG922A-CMW520-R1115	JG922A-CMW520-R1114			
JG923A-CMW52	JG923A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1115	R1114			
JG924A-CMW520-R1115	JG924A-CMW520-R1114			
JG925A-CMW520-R1115	JG925A-CMW520-R1114			
JG926A-CMW520-R1115	JG926A-CMW520-R1114			
JG927A-CMW520-R1115	JG927A-CMW520-R1114			
JG928A-CMW520-R1115	JG928A-CMW520-R1114			
JG920A-CMW520-R1114	JG920A-CMW520-R1113	2016-09-23	Release version	None
JG921A-CMW520-R1114	JG921A-CMW520-R1113			
JG922A-CMW520-R1114	JG922A-CMW520-R1113			
JG923A-CMW520-R1114	JG923A-CMW520-R1113			
JG924A-CMW520-R1114	JG924A-CMW520-R1113			
JG925A-CMW520-R1114	JG925A-CMW520-R1113			
JG926A-CMW520-R1114	JG926A-CMW520-R1113			
JG927A-CMW520-R1114	JG927A-CMW520-R1113			
JG928A-CMW520-R1114	JG928A-CMW520-R1113			
JG920A-CMW520-R1113	JG920A-CMW520-R1112	2016-06-28	Release version	This version fixed bugs and introduced feature changes. New features include: • Added IPv6 DHCP relay agent. • Added the management IP address and device MAC address fields to the **summary** command output.
JG921A-CMW520-R1113	JG921A-CMW520-R1112			
JG922A-CMW520-R1113	JG922A-CMW520-R1112			
JG923A-CMW520-R1113	JG923A-CMW520-R1112			
JG924A-CMW520-R1113	JG924A-CMW520-R1112			
JG925A-CMW520-R1113	JG925A-CMW520-R1112			
JG926A-CMW520-R1113	JG926A-CMW520-R1112			
JG927A-CMW520-R1113	JG927A-CMW520-R1112			
JG928A-CMW52	JG928A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1113	R1112			
JG920A-CMW520-R1112	JG920A-CMW520-R1111	2016-03-24	Release version	This version fixed bugs and introduced feature changes. New features include: • The device brand was changed from HP to HPE. • Configuring time zone and daylight saving time from the Web interface. • Configuring IPv6 ping and IPv6 traceroute from the Web interface.
JG921A-CMW520-R1112	JG921A-CMW520-R1111			
JG922A-CMW520-R1112	JG922A-CMW520-R1111			
JG923A-CMW520-R1112	JG923A-CMW520-R1111			
JG924A-CMW520-R1112	JG924A-CMW520-R1111			
JG925A-CMW520-R1112	JG925A-CMW520-R1111			
JG926A-CMW520-R1112	JG926A-CMW520-R1111			
JG927A-CMW520-R1112	JG927A-CMW520-R1111			
JG928A-CMW520-R1112	JG928A-CMW520-R1111			
JG920A-CMW520-R1111	JG920A-CMW520-R1110	2016-01-19	Release version	This version fixed bugs and introduced feature changes. New features include: You can enable the device to drop unknown multicast packets in the Web interface.
JG921A-CMW520-R1111	JG921A-CMW520-R1110			
JG922A-CMW520-R1111	JG922A-CMW520-R1110			
JG923A-CMW520-R1111	JG923A-CMW520-R1110			
JG924A-CMW520-R1111	JG924A-CMW520-R1110			
JG925A-CMW520-R1111	JG925A-CMW520-R1110			
JG926A-CMW520-R1111	JG926A-CMW520-R1110			
JG927A-CMW520-R1111	JG927A-CMW520-R1110			
JG928A-CMW520-R1111	JG928A-CMW520-R1110			
JG920A-CMW520-R1110	JG920A-CMW520-R1109	2015-12-23	Release version	None
JG921A-CMW520-R1110	JG921A-CMW520-R1109			
JG922A-CMW520-R1110	JG922A-CMW520-R1109			
JG923A-CMW520-R1110	JG923A-CMW520-R1109			
JG924A-CMW52	JG924A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1110	R1109			
JG925A-CMW520-R1110	JG925A-CMW520-R1109			
JG926A-CMW520-R1110	JG926A-CMW520-R1109			
JG927A-CMW520-R1110	JG927A-CMW520-R1109			
JG928A-CMW520-R1110	JG928A-CMW520-R1109			
JG920A-CMW520-R1109	JG920A-CMW520-R1108	2015-11-06	Release version	None
JG921A-CMW520-R1109	JG921A-CMW520-R1108			
JG922A-CMW520-R1109	JG922A-CMW520-R1108			
JG923A-CMW520-R1109	JG923A-CMW520-R1108			
JG924A-CMW520-R1109	JG924A-CMW520-R1108			
JG925A-CMW520-R1109	JG925A-CMW520-R1108			
JG926A-CMW520-R1109	JG926A-CMW520-R1108			
JG927A-CMW520-R1109	JG927A-CMW520-R1108			
JG928A-CMW520-R1109	JG928A-CMW520-R1108			
JG920A-CMW520-R1108	JG920A-CMW520-R1107	2015-08-06	Release version	None
JG921A-CMW520-R1108	JG921A-CMW520-R1107			
JG922A-CMW520-R1108	JG922A-CMW520-R1107			
JG923A-CMW520-R1108	JG923A-CMW520-R1107			
JG924A-CMW520-R1108	JG924A-CMW520-R1107			
JG925A-CMW520-R1108	JG925A-CMW520-R1107			
JG926A-CMW520-R1108	JG926A-CMW520-R1107			
JG927A-CMW520-R1108	JG927A-CMW520-R1107			
JG928A-CMW520-R1108	JG928A-CMW520-R1107			
JG920A-CMW52	JG920A-CMW520-	2015-05-05	Release	None

Version number	Last version	Release date	Release type	Remarks
0-R1107	R1106		version	
JG921A-CMW520-R1107	JG921A-CMW520-R1106			
JG922A-CMW520-R1107	JG922A-CMW520-R1106			
JG923A-CMW520-R1107	JG923A-CMW520-R1106			
JG924A-CMW520-R1107	JG924A-CMW520-R1106			
JG925A-CMW520-R1107	JG925A-CMW520-R1106			
JG926A-CMW520-R1107	JG926A-CMW520-R1106			
JG927A-CMW520-R1107	JG927A-CMW520-R1106			
JG928A-CMW520-R1107	JG928A-CMW520-R1106			
JG920A-CMW520-R1106	JG920A-CMW520-R1105	2015-03-17	Release version	None
JG921A-CMW520-R1106	JG921A-CMW520-R1105			
JG922A-CMW520-R1106	JG922A-CMW520-R1105			
JG923A-CMW520-R1106	JG923A-CMW520-R1105			
JG924A-CMW520-R1106	JG924A-CMW520-R1105			
JG925A-CMW520-R1106	JG925A-CMW520-R1105			
JG926A-CMW520-R1106	JG926A-CMW520-R1105			
JG927A-CMW520-R1106	JG927A-CMW520-R1105			
JG928A-CMW520-R1106	JG928A-CMW520-R1105			
JG920A-CMW520-R1105	JG920A-CMW520-R1104	2014-12-18	Release version	This version fixed bugs and introduced feature changes. New features include: GTS, For more information, see HPE1920-CMW520-R1105 Release Notes (Software Feature Changes). Modified features include: An ACL can be applied to multiple ports or VLANs.
JG921A-CMW520-R1105	JG921A-CMW520-R1104			
JG922A-CMW520-R1105	JG922A-CMW520-R1104			
JG923A-CMW520-R1105	JG923A-CMW520-R1104			
JG924A-CMW520-R1105	JG924A-CMW520-R1104			
JG925A-CMW52	JG925A-CMW520-			

Version number	Last version	Release date	Release type	Remarks
0-R1105	R1104			
JG926A-CMW520-R1105	JG926A-CMW520-R1104			
JG927A-CMW520-R1105	JG927A-CMW520-R1104			
JG928A-CMW520-R1105	First release			
JG920A-CMW520-R1104	JG920A-CMW520-R1103	2014-08-20	Release version	None
JG921A-CMW520-R1104	JG921A-CMW520-R1103			
JG922A-CMW520-R1104	JG922A-CMW520-R1103			
JG923A-CMW520-R1104	JG923A-CMW520-R1103			
JG924A-CMW520-R1104	JG924A-CMW520-R1103			
JG925A-CMW520-R1104	JG925A-CMW520-R1103			
JG926A-CMW520-R1104	JG926A-CMW520-R1103			
JG927A-CMW520-R1104	JG927A-CMW520-R1103			
JG920A-CMW520-R1103	JG920A-CMW520-R1102	2014-07-05	Release version	None
JG921A-CMW520-R1103	JG921A-CMW520-R1102			
JG922A-CMW520-R1103	JG922A-CMW520-R1102			
JG923A-CMW520-R1103	JG923A-CMW520-R1102			
JG924A-CMW520-R1103	JG924A-CMW520-R1102			
JG925A-CMW520-R1103	JG925A-CMW520-R1102			
JG926A-CMW520-R1103	JG926A-CMW520-R1102			
JG927A-CMW520-R1103	JG927A-CMW520-R1102			
JG920A-CMW520-R1102	First release	2014-06-07	Release version	None
JG921A-CMW520-R1102				
JG922A-CMW520-R1102				
JG923A-CMW52				

Version number	Last version	Release date	Release type	Remarks
0-R1102				
JG924A-CMW520-R1102				
JG925A-CMW520-R1102				
JG926A-CMW520-R1102				
JG927A-CMW520-R1102				

Hardware and software compatibility matrix

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	HPE OfficeConnect 1920 Switch Series
Memory	128MB
Flash	32 MB
Boot ROM version	Version 1.21 or higher (See **Note 2**)
Host software	JG920A-CMW520-R1121.bin JG921A-CMW520-R1121.bin JG922A-CMW520-R1121.bin JG923A-CMW520-R1121.bin JG924A-CMW520-R1121.bin JG925A-CMW520-R1121.bin JG926A-CMW520-R1121.bin JG927A-CMW520-R1121.bin JG928A-CMW520-R1121.bin
iMC version	iMC PLAT 7.3 (E0504P04) iMC EAD 7.3 (E0502) iMC EIA(TAM) 7.3 (E0503) iMC EIA(UAM) 7.3 (E0503)
iNode version	iNode 7.3 (E0504)

Display software and Boot ROM version information.

```
<HPE>summary
Vlan-interface:                 1

Select menu option:             Summary
IP Method:
IP address:
Subnet mask:
Default gateway:
```

```
IPv6 Method:
IPv6 link-local address:
IPv6 subnet mask length:
IPv6 global address:
IPv6 subnet mask length:
IPv6 default gateway:

Mac address: 0002-0133-D143

Current boot app is: flash:/hpe1920-8g.bin
Next main boot app is: flash:/hpe1920-8g.bin
Next backup boot app is: NULL

HPE Comware Platform Software
Comware Software, Version 5.20.99, Release 1121------------------- Note 1
Copyright (c) 2010-2019 Hewlett Packard Enterprise Development LP
HPE 1920-8G Switch uptime is 0 week, 0 day, 0 hour, 1 minute

HPE 1920-8G Switch
128M    bytes DRAM
32M     bytes Flash Memory
Config Register points to Flash

Hardware Version is Ver.A
Bootrom Version is 122----------------------Note 2
[SubSlot 0] 8GE+2SFP Hardware Version is Ver.A
```

Upgrading restrictions and guidelines

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

Hardware feature updates

None

Software feature and command updates

For more information about the software feature and command update history, see *HPE 1920-CMW520-R1121 Release Notes (Software Feature Changes).*

MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
CMW520-R1121			
New	None		None
Modified	None		None
CMW520-R1120			
New	None		None
Modified	None		None
CMW520-R1119			
New	None		None
Modified	None		None
CMW520-R1118			
New	None		None
Modified	None		None
CMW520-R1117			
New	None		None
Modified	None		None
CMW520-R1116			
New	None		None
Modified	None		None
CMW520-R1115			
New	None		None
Modified	None		None
CMW520-R1114			
New	None		None
Modified	None		None
CMW520-R1113			
New	None		None
Modified	None		None
CMW520-R1112			
New	None		None
Modified	None		None
CMW520-R1111			
New	None		None

Item	MIB file	Module	Description
Modified	None		None
CMW520-R1110			
New	None		None
Modified	None		None
CMW520-R1109			
New	None		None
Modified	None		None
CMW520-R1108			
New	None		None
Modified	None		None
CMW520-R1107			
New	None		None
Modified	None		None
CMW520-R1106			
New	None		None
Modified	None		None
CMW520-R1105			
New	None		None
Modified	None		None
CMW520-R1104			
New	None		None
Modified	None		None
CMW520-R1103			
New	None		None
Modified	None		None
CMW520-R1102			
New	None		First release
Modified	None		First release

Operation changes

None

Restrictions and cautions

- On the HPE1920 8G / HPE1920 8G PoE+ (65W) / HPE1920 8G PoE+ (180W) / HPE1920 16G / HPE1920 24G / HPE1920 24G PoE+ (180W) / HPE1920 24G PoE (370W) switches, do not configure a QoS policy with 802.1p priority marking and DSCP marking at the same time. If you configure both 802.1p priority marking and DSCP marking in a QoS policy, only DSCP marking takes effect.

- On the HPE1920 48G switch, a QoS policy does not support 802.1p priority marking or DSCP marking.
- If the number of IPv4 and IPv6 routes exceeds the upper limit, the exceeding routes are active but do not take effect.
- If the Admin Status is changed for IPv4 or IPv6 in the Modify page of VLAN Interface, the Admin Status is changed for both IPv4 and IPv6.
- The Ping, Loghost, and Trace Route functions in the Web interface cannot perform name resolution.
- The Temperature field displays 0°C because the device does not support temperature detection.
- After the device learns an ARP entry, a directly connected route and a MAC address entry will be added. The MAC address entry is added by the system, and is not limited by the MAC address learning limit set for an interface by using the mac-address max-mac-count command.
- The switch performs Layer 3 forwarding based on the hardware forwarding table and software ARP table. The switch preferentially uses the hardware forwarding table to direct Layer 3 forwarding. If the hardware resources are used up, the software ARP table is used. The hardware forwarding table provides much higher forwarding performance than the software ARP table. The hardware forwarding table resources of the switch are as follows:

Table 4 Table-Max hardware forwarding table resources for forwarding

HPE 1920 Switch Series Models	Max hardware forwarding table resources for forwarding
HPE 1920 8G Switch JG920A	60
HPE 1920 8G PoE+ (65W) Switch JG921A	60
HPE 1920 8G PoE+ (180W) Switch JG922A	60
HPE 1920 16G Switch JG923A	60
HPE 1920 24G Switch JG924A	60
HPE 1920 24G PoE+ (180W) Switch JG925A	60
HPE 1920 24G PoE+ (370W) Switch JG926A	60
HPE 1920 48G Switch JG927A	256
HPE 1920 48G PoE+ (370W) Switch JG928A	256

- The member ports of a Layer 2 aggregate interface cannot be used as stack ports.
- By default, the switch periodically sends cluster management protocol packets with the destination MAC address 01-80-C2-00-00-0A. A Cisco device might mistakenly recognize these packets as loop detection packets. As a result, the connecting interface on the Cisco device will be shut down. To solve this problem, perform the following tasks:
  - **a.** Export the switch's configuration file.
  - **b.** Edit the configuration file and add the following configuration to the configuration file:

    undo ndp enable

    undo ntdp enable

    undo cluster enable
  - **c.** Save the configuration file, and import the configuration file to the switch.

Open problems and workarounds

201303150291

- Symptom: When the storm control threshold is set in kbps or percentage, the storm control error is high for large-sized packets.
- Condition: None
- Workaround: Set the storm control threshold in pps.

201304020412

- Symptom: Storm suppression configured on an aggregation group member does not take effect.
- Condition: None
- Workaround: Configure storm suppression on the reference port of the aggregation group. The storm suppression configuration on the reference port suppresses traffic of the aggregation group.

201305300531

- Symptom: The MAC entry corresponding to a static ARP entry cannot be displayed.
- Condition: None
- Workaround: Configure a static MAC entry for the static ARP entry.

201307160332

- Symptom: A switch fails to route a packet that passes MAC authentication on the receiving interface.
- Condition: None
- Workaround: Configure MAC authentication on the access device and configure IP routing on the core device.

201306140403

- Symptom: When IGMP snooping or MLD snooping is enabled, well-known multicast protocol packets are forwarded according to multicast MAC entries.
- Condition: None
- Workaround: Disable IGMP snooping and MLD snooping.

List of resolved problems

Resolved problems in CMW520-R1121

201811280282

- Symptom: CVE-2017-12190
- Condition: An attacker can exploit this vulnerability to cause memory leak and possible system lockup.

Resolved problems in CMW520-R1120

201803060828

- Symptom: A memory leakage occurs on the HPE1920 device.
- Condition: This symptom occurs if you access the ipRouteEntry node by using SNMP and then specify a non-existent IP address or network segment for the ipRouteDest node.

Resolved problems in CMW520-R1119

201710250058

- Symptom: The Mitel VoIP phones attached to the device cannot automatically deploy the voice VLAN settings advertised by the device through LLDP.
- Condition: This symptom occurs if Mitel VoIP phones are attached to the device.

Resolved problems in CMW520-R1118

201706260084

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

Resolved problems in CMW520-R1117

201705060078

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

201706020564

- Symptom: The power that a PoE interface supplies to an Aruba AP might be insufficient.
- Condition: This symptom might occur if a PoE-capable device is connected to an Aruba AP and the cable is plugged/unplugged multiple times for the PoE interface connecting to the Aruba AP.

201706190111

- Symptom: When SNMP notifications are enabled and MIB node ifPhysAddress is read to query the MAC address of a VLAN interface, the MAC address is mistakenly displayed as 0000-0000-0000.
- Condition: This symptom might occur if SNMP notifications are enabled and MIB node ifPhysAddress is read to query the MAC address of a VLAN interface.

Resolved problems in CMW520-R1116

201612050267

- Symptom: CVE-2016-7427

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

201612050267

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

201703030296

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

201608290426

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

Resolved problems in CMW520-R1115

201609130118

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

201608310396

- Symptom: CVE-2014-9751
- Condition: The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly determine whether a source IP address is an IPv6 loopback address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.

Resolved problems in CMW520-R1114

201605160346

- Symptom: CVE-2016-1550
- Condition: Packet authentication tests have been performed using memcmp() or possibly bcmp(), and it is potentially possible for a local or perhaps LAN-based attacker to send a packet with an authentication payload and indirectly observe how much of the digest has matched.

201605160346

- Symptom: CVE-2016-1551

- Condition: While the majority OSes implement martian packet filtering in their network stack, at least regarding 127.0.0.0/8, a rare few will allow packets claiming to be from 127.0.0.0/8 that arrive over physical network. On these OSes, if ntpd is configured to use a reference clock an attacker can inject packets over the network that look like they are coming from that reference clock.

201605060556

- Symptom: CVE-2015-7973
- Condition: If an NTP network is configured for broadcast operations, then either a man-in-the-middle attacker or a malicious participant that has the same trusted keys as the victim can replay time packets.

201605060556

- Symptom: CVE-2015-7974
- Condition: Symmetric key encryption uses a shared trusted key. The reported title for this issue was "Missing key check allows impersonation between authenticated peers" and the report claimed "A key specified only for one server should only work to authenticate that server, other trusted keys should be refused." Except there has never been any correlation between this trusted key and server v. clients machines and there has never been any way to specify a key only for one server. We have treated this as an enhancement request, and ntp-4.2.8p6 includes other checks and tests to strengthen clients against attacks coming from broadcast servers.

201607040231

- Symptom: CVE-2016-4954
- Condition: An attacker who is able to spoof packets with correct origin timestamps from enough servers before the expected response packets arrive at the target machine can affect some peer variables and, for example, cause a false leap indication to be set.

201608290268

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in drivers/char/random.c in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms based on randomization, via vectors that leverage the function's tendency to "return the same value over and over again for long stretches of time."

201607290082

- Symptom: CVE-2016-1409
- Condition: The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Cisco IOS XE 2.1 through 3.17S, IOS XR 2.0.0 through 5.3.2, and NX-OS allows remote attackers to cause a denial of service (packet-processing outage) via crafted ND messages, aka Bug ID CSCuz66542, as exploited in the wild in May 2016.

201608080266

- Symptom: The device cannot establish LLDP neighbor relationship with a Cisco device if the Cisco device does not have an IP address.
- Condition: This symptom occurs if the device is enabled with CDP compatibility and works with the Cisco device enabled with CDP.

201609060484

- Symptom: The operations of the MDI mode and the MDIX mode of an Ethernet interface are reverse.
- Condition: None

201608240400

- Symptom: The MDI mode cannot be set for an Ethernet interface whose physical link state is up.
- Condition: This symptom occurs on a device that does not support PoE.

Resolved problems in CMW520-R1113

None

Resolved problems in CMW520-R1112

201512280218

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

Resolved problems in CMW520-R1111

201512150189

- Symptom: Failure to access the device by using the Chrome browser through the HTTPS protocol.
- Condition: This symptom occurs if the latest Chrome browser is used to access the device through the HTTPS protocol.

Resolved problems in CMW520-R1110

201511190277

- Symptom: The switch keeps sending ARP requests to the connected VRRP group.
- Condition: This symptom might occur if load sharing is enabled for the VRRP group, and the switch is assigned the virtual MAC address of a backup gateway in the VRRP group.

Resolved problems in CMW520-R1109

201510210531

- Symptom: The MAC addresses obtained by an NMS are incomplete.
- Condition: This symptom might occur if multiple NMSs access the public MIB node dot1pTpFdbAddressdot1 (OID is 1.3.6.1.2.1.17.7.1.2.2.1.2) to obtain the MAC addresses of the switches.

201507160257

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

201507160257

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

201507160257

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

Resolved problems in CMW520-R1108

201507210233

- Symptom: The flash area for storing log files might be destroyed by frequent write actions. As a result, the switch fails and cannot start up.
- Condition: The log file feature is enabled on the switch. Logs are frequently updated for a long period of time.

201507070204

- Symptom: When the switch starts, the switch cannot obtain a configuration file through the TFTP server configured on the DHCP server.
- Condition: Start the switch without any configuration.

201504070120

- Symptom: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Such reuse is and has been strongly discouraged and is believed to be rare. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected. Certificate parsing (d2i_X509 and related functions) are however not affected. OpenSSL clients and servers are not affected.

201504070120

- 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. Applications that verify PKCS#7 signatures, decrypt PKCS#7 data or otherwise parse PKCS#7 structures from untrusted sources are affected. OpenSSL clients and servers are not affected.

201504070120

- Symptom: CVE-2015-0292
- Condition: A vulnerability existed in previous versions of OpenSSL related to the processing of base64 encoded data. Any code path that reads base64 data from an untrusted source could be affected (such as the PEM processing routines). Maliciously crafted base 64 data could trigger a segmenation fault or memory corruption. This was addressed in previous versions of OpenSSL but has not been included in any security advisory until now.

201504070120

- 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, in turn, could cause a double free in several private key parsing functions (such as d2i_PrivateKey or EVP_PKCS82PKEY) and could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources. This scenario is considered rare.

201504070120

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

Resolved problems in CMW520-R1107

201503030188

- 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.

201503030188

- 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.

201503030188

- 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.

201503030188

- 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.

201503030188

- 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.

201503030188

- 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 CMW520-R1106

201412310265

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

Resolved problems in CMW520-R1105

201408280092

- Symptom: CVE-2008-5161.
- Condition: 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.

201408150032

- 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.

201410220283

- 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).

Resolved problems in CMW520-R1104

201408150484

- Symptom: If an aggregate interface receives a unicast ARP packet destined to the aggregate interface, it sends the ARP packet out.
- Condition: This symptom can be seen if the VLAN of the aggregate interface is enabled with ARP detection.

Resolved problems in CMW520-R1103

201406100576

- Symptom: CVE-2014-0224.

- Condition: When Open SSL Server is used.

Resolved problems in CMW520-R1102

First release

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect:

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

Documents

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

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

Related documents

The following documents provide related information:

- HPE OfficeConnect 1920 Switch Series Getting Started Guide
- HPE OfficeConnect 1920 Switch Series User Guide

Documentation feedback

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

Appendix A Feature list

Hardware features

Table 5 HPE OfficeConnect 1920 Switch Series hardware features

Item	HPE1920 8G	HPE1920 16G	HPE1920 24G	HPE1920 48G
Dimensions (H × W × D)	44 x 266 x 162 mm (1.73 x 10.47 x 6.38 in)	44 x 440 x 173 mm (1.73 x 17.32 x 6.81 in)	44 x 440 x 173 mm (1.73 x 17.32 x 6.81 in)	44 x 440 x 238 mm (1.73 x 17.32 x 9.37 in)
Switching capacity	192Gbps			240Gbps
Throughput	14.8Mpps	29.6Mpps	41.7Mpps	77.4Mpps
Ports	8 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 2 100/1000Base-X SFP ports	16 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 4 100/1000Base-X SFP ports	24 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 4 100/1000Base-X SFP ports	48 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 4 100/1000Base-X SFP ports
SFP	Support 1000BASE-X SFP Support 100BASE-X SFP			
PoE	Not supported			
Temperature	Operating temperature: 0 °C to 40°C Storage temperature: -40 °C to 70 °C			
Humidity	Operating relative humidity: 5% to 95%, noncondensing Storage relative humidity: 5% to 95%, noncondensing			
Emissions	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A,			
Safety	EN60950-1, UL 60950-1 2nd edition / CSA22.2 No 60950-1 2nd edition, IEC 60950-1			
Max power	≤ 8.5 W	≤ 13 W	≤ 19W	≤32W
Weight	≤ 1 kg (2.20 lb)	≤ 2.1 kg (4.63 lb)	≤ 2.2 kg (4.85 lb)	≤ 3.4 kg (7.50 lb)
Input AC Voltage	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz or 60 Hz			

Item	HPE1920 8G PoE+ (65W)	HPE1920 8G PoE+ (180W)	HPE1920 24G PoE+ (180W)	HPE1920 24G PoE+ (370W)	HPE1920 48 PoE+ (370W)
Dimensions (H × W × D)	44 x 330 x 230 mm (1.73 x 12.99 x 9.06 in)	44 x 330 x 230 mm (1.73 x 12.99 x 9.06 in)	44 x 440 x 238 mm (1.73 x 17.32 x 9.37 in)	44 x 440 x 260 mm (1.73 x 17.32 x 10.24 in)	44 x 440 x 400 mm (1.73 x 17.32 x 15.75 in)

Item	HPE1920 8G PoE+ (65W）	HPE1920 8G PoE+ (180W)	HPE1920 24G PoE+ (180W)	HPE1920 24G PoE+ (370W)	HPE1920 48 PoE+ (370W)
Switching capacity	192Gbps				240Gbps
Throughput	14.8Mpps		41.7Mpps		77.4Mpps
Ports	8 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 2 100/1000Base-X SFP ports		24 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 4 100/1000Base-X SFP ports		48 RJ-45 auto-negotiating 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX 802.3ab Type 1000BASE-TX) 4 100/1000Base-X SFP ports
SFP	Support 1000BASE-X SFP Support 100BASE-X SFP				
PoE	A single PoE port provides power consumption up to 30 W and the switch provides up to 65 W for PoE port-connected devices in total.	A single PoE port provides power consumption up to 30 W and the switch provides up to 180 W for PoE port-connected devices in total.	A single PoE port provides power consumption up to 30 W and the switch provides up to 180 W for PoE port-connected devices in total.	A single PoE port provides power consumption up to 30 W and the switch provides up to 370 W at AC input 740 W at RPS DC input for PoE port-connected devices in total.	A single PoE port provides power consumption up to 30 W and the switch provides up to 370 W at AC input 740 W at RPS DC input for PoE port-connected devices in total.
Temperature	Operating temperature: 0 °C to 40°C Storage temperature: -40 °C to 70°C				
Humidity	Operating relative humidity: 5% to 95%, noncondensing Storage relative humidity: 5% to 95%, noncondensing				
Emissions	FCC part 15 Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; EN 55024; EN 61000-3-2 2000, 61000-3-3; ICES-003 Class A,				
Safety	EN60950-1, UL 60950-1 2nd edition / CSA22.2 No 60950-1 2nd edition, IEC 60950-1				
Max power	≤ 94 W	≤ 230 W	≤ 235 W	474 W at AC input 834 W at RPS DC input	492 W at AC input 876 W at RPS DC input
Weight	≤ 2.1 kg (4.63 lb)	≤ 2.5 kg (5.51 lb)	≤ 3.4 kg (7.50 lb)	≤ 4.0 kg (8.82 lb)	≤ 6.0 kg (13.23 lb)
Input AC Voltage	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz or 60 Hz				

Software features

Table 6 Software features of the HPE OfficeConnect 1920 Switch Series

Item	HPE1920 8G	HPE1920 8G PoE+ (65W）	HPE1920 8G PoE+ (180W)	HPE1920 16G	HPE1920 24G	HPE1920 24G PoE+ (180W)	HPE1920 24G PoE+ (370W)	HPE1920 48G	HPE1920 48G PoE+ (370W)
VLAN	Voice VLAN								
IPv4	Static routing (32)								
IPv6	IPv6 routing (32) ND Pingv6, Telnetv6, FTPv6, TFTPv6, ICMPv6								
DHCP	DHCP relay DHCP client DHCP snooping DHCP snooping Option 82								
Multicast	IGMP V1/V2/V3 snooping MLD V1/V2 snooping								
ACL	Mac based and IP based ACL Ingress ACL								
QoS	Diff-Serv QoS SP/WRR/SP+WRR queue schedule Priority mark/remark								
security	Two-level admin and monitor management SSHv2 ARP anti-attack MAC limit IEEE 802.1X RADIUS SNMPv3, SSHv2 Broadcast storm control								
System management	Console/AUX Modem/Telnet/SSH2.0 command line configuration FTP, TFTP, XModem, SFTP software application file download SNMP V1/V2c/V3 RMON, 1, 2, 3, 9 group NTP Syslog single IP management (IRF-Lite)								

Item	HPE1920 8G	HPE1920 8G PoE+ (65W）	HPE1920 8G PoE+ (180W)	HPE1920 16G	HPE1920 24G	HPE1920 24G PoE+ (180W)	HPE1920 24G PoE+ (370W)	HPE1920 48G	HPE1920 48G PoE+ (370W)
PoE	Not supported	PoE Power 65W Port Max 30W	PoE Power 180W Port Max 30W	Not supported	Not supported	PoE Power 180W Port Max 30W	PoE Power 370 W at AC input 740 W at RPS DC input Port Max 30W	Not supported	PoE Power 370 W at AC input 740 W at RPS DC input Port Max 30W

Appendix B Upgrading software

This section describes how to upgrade system software while the switch is operating normally or when the switch cannot correctly start up.

System software file types

System software images are in .bin format (for example, main.bin) and run at startup. You can set a system software image as a **main**, **backup**, or **secure** image.

At startup, the switch always attempts to boot first with the main system software image. If the attempt fails, for example, because the image file is corrupted, the switch tries to boot with the backup system software image. If the attempt still fails, the switch tries to boot with the secure system software image. If all attempts fail, the switch displays a failure message.

Upgrade methods

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

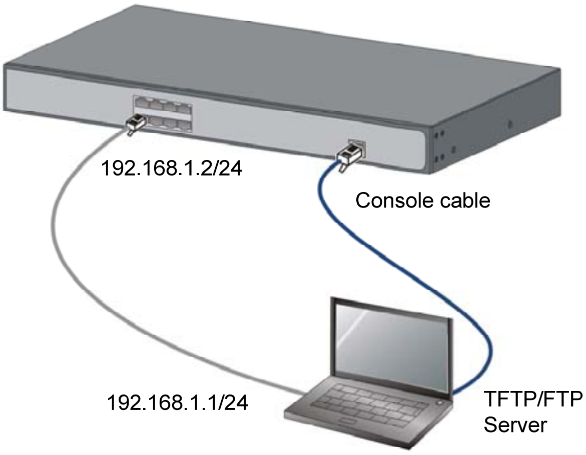
Upgrade method	Remarks
Upgrading from the WEB	• You must reboot the switch to complete the upgrade. • This method can interrupt ongoing network services.
Upgrading from the BootWare menu	Use this method when the switch cannot correctly start up.

Preparing for the upgrade

Before you upgrade system software, complete the following tasks:

- Set up the upgrade environment as shown in Table 8.
- Configure switch to make sure that the switch and the file server can reach each other.
- Run a TFTP or FTP server on the file server.
- Log in to the CLI of the switch through the console port.
- Copy the upgrade file to the file server and correctly set the working directory on the TFTP or FTP server.
- Make sure that the upgrade has minimal impact on the network services. During the upgrade, the switch cannot provide any services.

Figure 1 Set up the upgrade environment

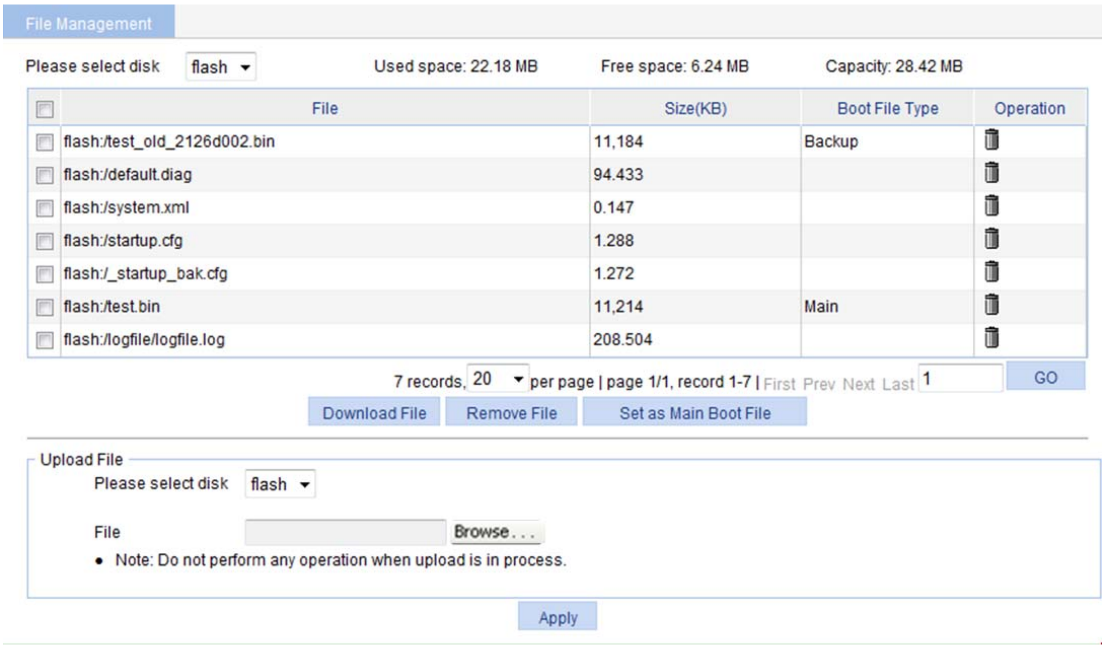


Upgrading from the WEB

Upgrading the system software

1. Select **Device** > **File Management** from the navigation tree to enter the file management page, as shown in Figure 2 .

Figure 2 File management



Please select disk flash Used space: 22.18 MB Free space: 6.24 MB Capacity: 28.42 MB

□	File	Size(KB)	Boot File Type	Operation
□	flash:/test_old_2126d002.bin	11,184	Backup	🗑
□	flash:/default.diag	94.433		🗑
□	flash:/system.xml	0.147		🗑
□	flash:/startup.cfg	1.288		🗑
□	flash:/_startup_bak.cfg	1.272		🗑
□	flash:/test.bin	11,214	Main	🗑
□	flash:/logfile/logfile.log	208.504		🗑

7 records, 20 per page | page 1/1, record 1-7 | First Prev Next Last 1

Upload File

Please select disk flash

File

- Note: Do not perform any operation when upload is in process.

2. In the **Upload File** area, select a disk from the **Please select disk** drop-down list to save the file, and then select the file path and filename by clicking **Browse**. Click **Apply** to upload the file to the specified storage device.
3. Select the application file (with the extension.bin or .app) from the file list.
4. Click Set as Main Boot File

CAUTION:

Uploading a file takes some time. Hewlett Packard Enterprise recommends you not to perform any operation on the web interface during the upgrading procedure.

Upgrading from the BootWare menu

You can use one of the following methods to upgrade software from the BootWare menu:

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

TIP:

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

Accessing the BootWare menu

1. Power on the switch (for example, an HPE1920 8G), and you can see the following information:

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU
Booting Normal Extend BootWare
The Extend BootWare is self-decompressing.....................Done!

****************************************************************************
*                                                                          *
*             HPE 1920-8G Switch JG920A BootWare, Version 1.22              *
*                                                                          *
****************************************************************************
Copyright (c) 2010-2017 Hewlett Packard Enterprise Development LP

Compiled Date       : Apr 14 2017 15:05:19
CPU Type            : MIPS4kec
CPU L1 Cache        : 16KB
CPU Clock Speed     : 650MHz
Memory Type         : DDR3 SDRAM
Memory Size         : 128MB
Memory Speed        : 300MHz
BootWare Size       : 3MB
Flash Size          : 32MB


BootWare Validating...
Press Ctrl+B to enter extended boot menu...
```

2. Press **Ctrl + B** at the prompt.

```
BootWare password: Not required. Please press Enter to continue.

Password recovery capability is enabled.
Note: The current operating device is flash
```

```
Enter < Storage Device Operation > to select device.

===========================<EXTEND-BOOTWARE MENU>===========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
|<4> File Control                                                          |
|<5> Restore to Factory Default Configuration                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Clear Super Password                                                  |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
============================================================================
Ctrl+Z: Access EXTEND-ASSISTANT MENU
Ctrl+F: Format File System
Ctrl+C: Display Copyright
Enter your choice(0-9):
```

Table 7 BootWare menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 11) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 9) for upgrading system software through an Ethernet port or changing Ethernet settings.
<4> File Control	Access the File Control submenu (see Table 12) to retrieve and manage the files stored on the switch.
<5> Restore to Factory Default Configuration	Restore to Factory Default Configuration
<6> Skip Current System Configuration	Start the switch with the factory default configuration. This is a one-time operation and does not take effect at the next reboot. You use this option when you forget the console login password.
<7> BootWare Operation Menu	Access the BootWare Operation menu for backing up, restoring, or upgrading BootWare. When you upgrade the system software image, BootWare is automatically upgraded. HPE does not recommend upgrading BootWare separately. This document does not cover using the BootWare Operation menu.
<8> Clear Super Password	Clear all super passwords used for switching to higher user privilege levels. By default, no super password is required for switching to a higher user privilege level.
<9> Storage Device Operation	Access the Storage Device Operation menu to manage storage devices. Using this option is beyond this chapter.
<0> Reboot	Restart the switch.

Using TFTP/FTP to upgrade software through an Ethernet port

1. Enter **3** in the BootWare menu to access the Ethernet submenu.

```
=========================<Enter Ethernet SubMenu>=========================
|Note:the operating device is cfa0                                         |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
==========================================================================
Enter your choice(0-5):
```

Table 8 Ethernet submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM and run the image.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.
<4> Update Secure Application File	Upgrade the secure system software image.
<5> Modify Ethernet Parameter	Modify network settings.
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter **5** to configure the network settings.

```
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|          Ctrl+D = Quit.                                                  |
==========================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :main.bin
                       :
Target File Name       :main.bin
                       :
Server IP Address      :192.168.1.1
Local IP Address       :192.168.1.253
Gateway IP Address     :0.0.0.0
FTP User Name          :user
FTP User Password      :password
```

Table 9 Network parameter fields and shortcut keys

Field	Description
'.' = Clear field	Press a dot (.) and then **Enter** to clear the setting for a field.

Field	Description
'-' = Go to previous field	Press a hyphen (-) and then **Enter** to return to the previous field.
Ctrl+D = Quit	Press **Ctrl** + **D** to exit the Ethernet Parameter Set menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP or TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file on the switch. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP or TFTP server. If a mask must be set, use a colon (:) to separate the mask length from the IP address. For example, 192.168.80.10:24.
Local IP Address	Set the IP address of the switch.
Gateway IP Address	Set a gateway IP address if the switch is on a different network than the server.
FTP User Name	Set the username for accessing the FTP server. This username must be the same as configured on the FTP server. This field is not available for TFTP.
FTP User Password	Set the password for accessing the FTP server. This password must be the same as configured on the FTP server. This field is not available for TFTP.

3. Select an option in the Ethernet submenu to upgrade a system software image. For example, enter **2** to upgrade the main system software image.

```
Loading....................................................................
...........................................................................
.........................Done!
12521472 bytes downloaded!
Updating File flash:/main.bin..............................................
...................................................Done!
=========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                       |
|<1> Download Application Program To SDRAM And Run                        |
|<2> Update Main Application File                                         |
|<3> Update Backup Application File                                       |
|<4> Update Secure Application File                                       |
|<5> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
|<Ensure The Parameter Be Modified Before Downloading!>                   |
===========================================================================
Enter your choice(0-5):
```

4. Enter **0** to return to the BootWare menu.
5. In the BootWare menu, enter **1** to boot the system.

Using XMODEM to upgrade software through the console port

1. Enter **2** in the BootWare menu to access the Serial submenu.

```
==========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-5):
```

Table 10 Serial submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download an application to SDRAM through the serial port and run the program.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.
<4> Update Secure Application File	Upgrade the secure system software image.
<5> Modify Serial Interface Parameter	Modify serial port parameters
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter **5** to modify serial interface parameters.
3. Select an appropriate baud rate for the console port. For example, enter **5** to select 115200 bps.

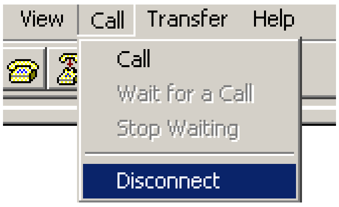
```
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>---------------------------|
|<1> 9600                                                         |
|<2> 19200                                                                 |
|<3> 38400 (Default)*                                                           |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):5
The following messages appear:
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

NOTE:

Typically the size of a .bin file is over 10 MB. Even at 115200 bps, the download takes about 30 minutes.

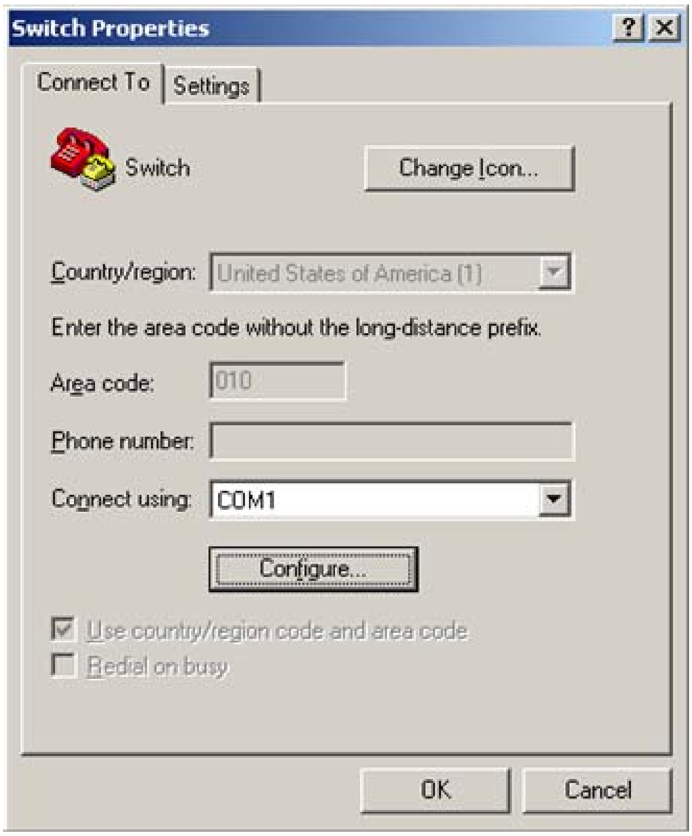
4. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 3 Disconnect the terminal connection



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

Figure 4 Properties dialog box



Switch

Country/region: United States of America (1)

Enter the area code without the long-distance prefix.

Area code: 010

Phone number:

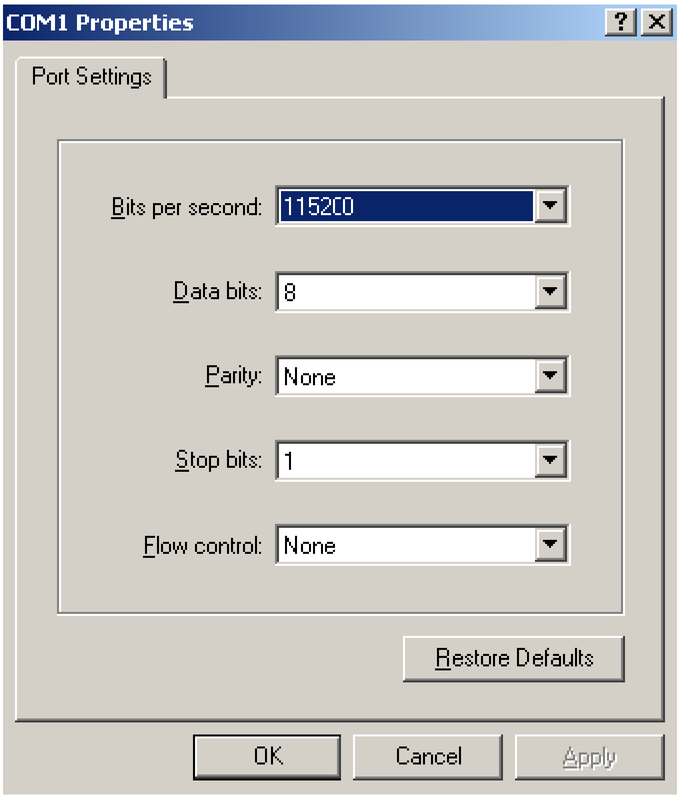
Connect using: COM1

☑ Use country/region code and area code

□ Redial on busy

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

Figure 5 Modify the baud rate


COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

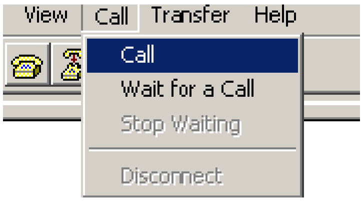
Parity: None

Stop bits: 1

Flow control: None

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

Figure 6 Reestablish the connection



8. Press **Enter**.

   The following menu appears:

```
The current baudrate is 115200 bps
===============================<BAUDRATE SET>===============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>---------------------------|
|<1> 9600                                                         |
|<2> 19200                                                                |
|<3> 38400(Default)                                                             |
|<4> 57600                                                                 |
|<5> 115200*                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

9. Enter **0** to return to the Serial submenu.

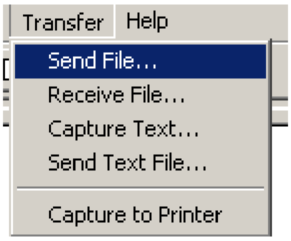
```
===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-5):
```

10. Select an option from options **2** to **4** to upgrade a system software image. For example, enter **2** to upgrade the main system software image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

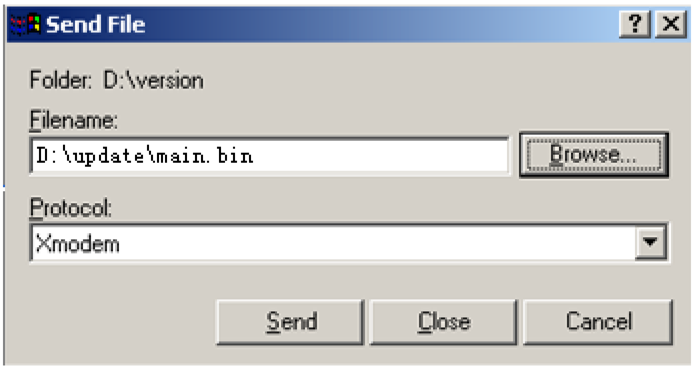
11. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 7 Transfer menu



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

Figure 8 File transmission dialog box



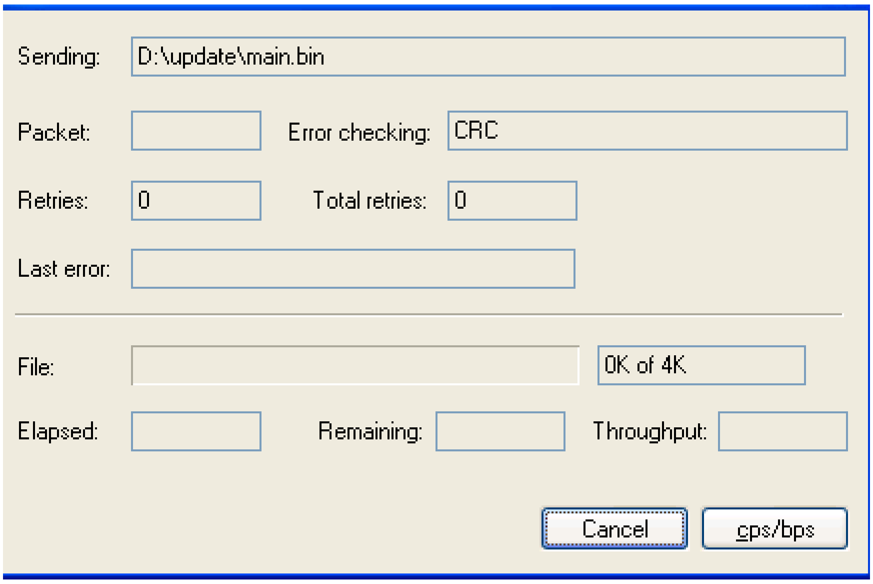
Folder: D:\version

Filename: D:\update\main.bin

Protocol: Xmodem

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

Figure 9 File transfer progress



Sending: D:\update\main.bin

Packet:

Error checking: CRC

Retries: 0

Total retries: 0

Last error:

File: 0K of 4K

Elapsed:

Remaining:

Throughput:

14. When the Serial submenu appears after the file transfer is complete, enter **0** at the prompt to return to the BootWare menu.

```
Download successfully!
31911808 bytes downloaded!
Input the File Name:main.bin
Updating File flash:/main.bin..............................................
.....................................................Done!

===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                       |
|<1> Download Application Program To SDRAM And Run                        |
|<2> Update Main Application File                                         |
|<3> Update Backup Application File                                       |
|<4> Update Secure Application File                                       |
|<5> Modify Serial Interface Parameter                                    |
|<0> Exit To Main Menu                                                    |
============================================================================
Enter your choice(0-5):
```

15. Enter **1** in the BootWare menu to boot the system.
16. If you are using a download rate other than 38400 bps, change the baud rate of the terminal to 38400 bps. If the baud rate has been set to 38400 bps, skip this step.

Managing files from the BootWare menu

To change the type of a system software image, retrieve files, or delete files, enter **4** in the BootWare menu.

The File Control submenu appears:

```
==============================<File CONTROL>==============================
|Note:the operating device is flash                                      |
|<1> Display All File(s)                                                |
|<2> Set Application File type                                          |
|<3> Set Configuration File type                                        |
|<4> Delete File                                                        |
|<0> Exit To Main Menu                                                  |
==========================================================================
Enter your choice(0-4):
```

Table 11 File Control submenu options

Item	Description
<1> Display All File	Display all files.
<2> Set Application File type	Change the type of a system software image.
<3> Set Configuration File type	Change the type of a configuration file.
<4> Delete File	Delete files.
<0> Exit To Main Menu	Return to the BootWare menu.

Displaying all files

To display all files, enter **1** in the File Control submenu:

```
Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==========================================================================
|NO. Size(B)   Time                 Type   Name                         |
|1   640199    Dec/20/2012 09:53:16 N/A    flash:/logfile/logfile.log     |
|2   22165484  Dec/20/2012 09:18:10 B+S    flash:/update.bin              |
|3   1181      Dec/20/2012 09:42:54 N/A    flash:/startup.cfg             |
|4   22165484  Dec/20/2012 09:42:28 M      flash:/main.bin                |
==========================================================================
```

Changing the type of a system software image

System software image file attributes include main (M), backup (B), and secure (S). You can store only one main image, one backup image, and one secure image on the switch. A system software image can have any combination of the M, B, and S attributes. If the file attribute you are assigning has been assigned to an image, the assignment removes the attribute from that image. The image is marked as N/A if it has only that attribute.

For example, the file main.bin has the M attribute and the file update.bin has the S attribute. After you assign the M attribute to update.bin, the type of update.bin changes to M+S and the type of main.bin changes to N/A.

NOTE:

You cannot remove or assign the S attribute in the File Control submenu.

To change the type of a system software image:

1. Enter **2** in the File Control submenu.

```
'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==========================================================================
|NO. Size(B)   Time                 Type   Name                         |
|1   22165484  Dec/20/2012 09:18:10 B+S    flash:/update.bin              |
|2   22165484  Dec/20/2012 09:42:28 M      flash:/main.bin                |
|0   Exit                                                                |
========================================================================
Enter file No:
```

2. Enter the number of the file you are working with, and press **Enter**.

```
Modify the file attribute:
==========================================================================
|<1> +Main                                                               |
|<2> -Main                                                               |
|<3> +Backup                                                             |
|<4> -Backup                                                             |
|<0> Exit                                                                |
==========================================================================
Enter your choice(0-4):
```

3. Enter a number in the range of 1 to 4 to add or delete a file attribute for the file.

```
Set the file attribute success!
```

Deleting files

When storage space is insufficient, you can delete obsolete files to free up storage space.

To delete files:

1. Enter **4** in the File Control submenu.

```
Deleting the file in cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==========================================================================
|NO. Size(B)   Time                 Type   Name                          |
|1   640199    Dec/20/2012 09:53:16 N/A    flash:/logfile/logfile.log     |
|2   22165484  Dec/20/2012 09:18:10 B+S    flash:/update.bin              |
|3   1181      Dec/20/2012 09:42:54 N/A    flash:/startup.cfg             |
|4   22165484  Dec/20/202 09:42:28 M      flash:/main.bin                 |
|0   Exit                                                                |
==========================================================================
Enter file No:
```

2. Enter the number of the file to delete.
3. When the following prompt appears, enter **Y**.

```
The file you selected is cfa0:/backup.bak,Delete it? [Y/N]Y
Deleting........Done!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version. To handle a software failure:

1. Check the physical ports for a loose or incorrect connection.
2. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
3. Check the file transfer settings:

  - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
  - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
  - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.

4. Check the FTP or TFTP server for any incorrect setting.
5. Check that the storage device has sufficient space for the upgrade file.
6. If the message “Something is wrong with the file” appears, check the file for file corruption.

Hewlett Packard
Enterprise

HPE1920-CMW520-R1120 Release Notes Software Feature Changes

Contents

Release HPE 1920-CMW520-R1121 1

Release HPE 1920-CMW520-R1120 2

Release HPE 1920-CMW520-R1119 3

Modified feature: Configuring the Port ID Subtype field in the Port ID TLV through the Web interface 3

Feature change description 3

Configuring the Port ID Subtype field in the Port ID TLV through the Web interface 3

Release HPE 1920-CMW520-R1118 5

Related documentation 6

Release HPE 1920-CMW520-R1121

This release has no feature changes.

Release HPE 1920-CMW520-R1120

This release has no feature changes.

Release HPE 1920-CMW520-R1119

This release has the following changes:

- Modified feature: Configuring the Port ID Subtype field in the Port ID TLV through the Web interface

Modified feature: Configuring the Port ID Subtype field in the Port ID TLV through the Web interface

Feature change description

In previous software versions, the port ID subtype field in the port ID TLV takes either of the following values by default and cannot be changed:

- If the LLDPDU contains an LLDP-MED TLV, the port ID subtype field displays the MAC address of the outgoing interface. If the interface does not have a MAC address, the bridge MAC address is displayed.
- If the LLDPDU does not contain an LLDP-MED TLV, the port ID subtype field displays the name of the outgoing interface.

This software version allows you to configure the port ID subtype field in the port ID TLV to take any of the following values:

- Default.
- Interface alias.
- Interface name.
- Locally assigned.

Configuring the Port ID Subtype field in the Port ID TLV through the Web interface

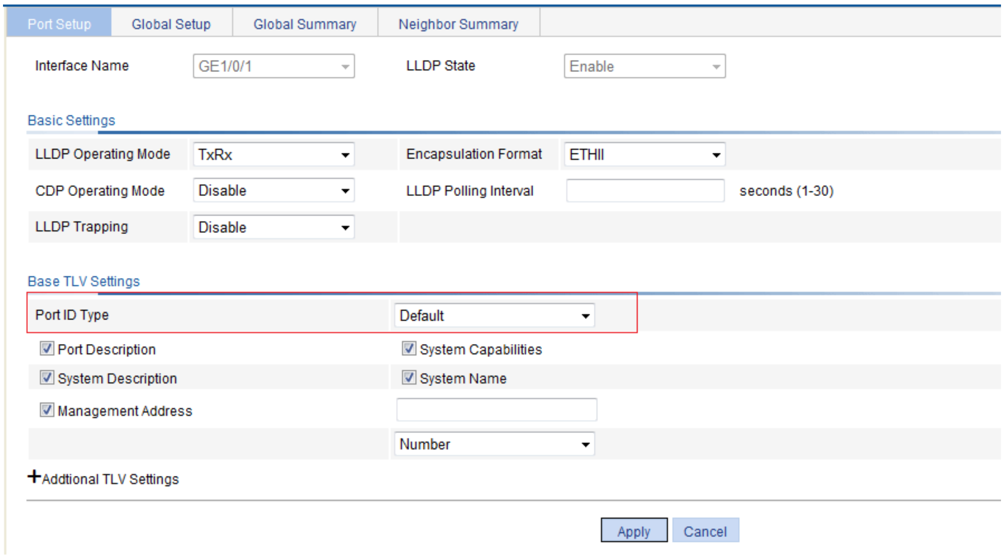
1. From the navigation tree, select **Network** > **LLDP**.

   By default, the **Port Setup** tab is displayed.

2. Click the icon for a port.

   On the page as shown in Figure 1, the LLDP settings of the port are displayed.

Figure 1 Configuring the Port ID Type



Interface Name: GE1/0/1

LLDP State: Enable

Basic Settings

LLDP Operating Mode: TxRx

Encapsulation Format: ETHII

CDP Operating Mode: Disable

LLDP Polling Interval: seconds (1-30)

LLDP Trapping: Disable

Base TLV Settings

Port ID Type: Default

☑ Port Description

☑ System Capabilities

☑ System Description

☑ System Name

☑ Management Address

Number

+Addtional TLV Settings

3. Select the type of value the port ID subtype field uses from the **Port ID Type** list. See Table 1 for the available options.
4. Click **Apply**.

   A progress dialog box appears.
3. Click **Close** on the progress dialog box when the progress dialog box prompts that the configuration succeeds.

Table 1 Configuration items

Port ID Type	Default	Use the default settings: • If the LLDPDU contains an LLDP-MED TLV, the MAC address of the outgoing interface is used. If the interface does not have a MAC address, the bridge MAC address is used. • If the LLDPDU does not contain an LLDP-MED TLV, the name of the outgoing interface is used as the port ID subtype.
	Interface alias	Use the interface alias.
	Interface name	Use the interface name.
	Locally assigned	Use the locally assigned interface name.

Release HPE 1920-CMW520-R1118

This release has no feature changes.

Related documentation

This document introduces software feature before HPE OfficeConnect 1920 Switch Series CMW520-R1117 versions please refer to *HPE OfficeConnect 1920 Switch Series User Guide.*