HP 8/20q Fibre Channel Switch Installation and Reference Guide

This guide describes the HP 8/20q Fibre Channel Switch features and capabilities, planning considerations, installation, diagnostics, and troubleshooting. This guide is intended for users who are responsible for installing and servicing network equipment.

Part number: 5697-2288
Published November 2012
Edition: 7

Legal and notice information

© Copyright 2008, 2012 Hewlett-Packard Development Company, L.P.

© Copyright 2008-2012 This software includes technology under a license from QLogic Corporation. All rights reserved.

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.

WARRANTY STATEMENT: To obtain a copy of the warranty for this product, see the warranty information website: http://www.hp.com/go/storagewarranty.

Java is a registered trademark of Sun Microsystems, Inc.

Microsoft, Windows XP, and Windows 2000/2003, and Internet Explorer are registered trademarks of Microsoft Corporation.

Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.

HP 8/20q Fibre Channel Switch Installation and Reference Guide

Contents

1 General Description 7
Switch LEDs and controls 8
Input power LED (green) 8
Heartbeat LED (green) 8
System fault LED (amber) 8
Maintenance button 9
Resetting a switch 9
Placing the switch in maintenance mode 9
Fibre Channel ports 10
Port LEDs 10
Port Logged-in LED (green) 10
Port Activity LED (green) 11
Transceivers 11
Port types 11
Ethernet port 12
Serial port 12
Power supply and fans 13
Switch management 13
QuickTools web applet 14
SAN Connection Manager 14
Command line interface 14
Enterprise Fabric Management Suite 14
Simple Network Management Protocol 14
Storage Management Initiative–Specification (SMI-S) 15
File transfer protocols 15

2 Planning a Fabric 17
Devices 17
Device access 17
Performance 18
Distance 18
Bandwidth 19
Latency 19
Feature licenses 20
Multiple switch fabrics 20
Optimizing device performance 20
Domain ID, principal priority, and domain ID lock 21
Common topologies 21
Transparent routing 21
Switch services 23
Security 25
User account security 25
IP security 25
Port binding 26
Connection security 26
Device security 26
Fabric management 27

3 Installation 29
Site requirements 29
Management Station and Workstation requirements 29
Switch power requirements 30
Environmental conditions 30
Installing a switch 30

Mount the switch . . . 31
Before you begin . . . 31
Collect the required items . . . 32
Verify the kit contents . . . 32
Rack the switch . . . 33
Install the transceivers . . . 35
Configure the workstation . . . 35
Configuring the workstation IP address for Ethernet connections . . . 35
Configuring the workstation serial port . . . 35
Apply power to the switch . . . 36
Connect the management station or workstation to the switch . . . 37
Configure the switch . . . 37
SAN Connection Manager switch configuration . . . 37
QuickTools switch configuration . . . 38
Enterprise Fabric Management Suite configuration . . . 38
CLI switch configuration . . . 38
Cable devices to the switch . . . 39
Installing firmware . . . 39
Using QuickTools to install firmware . . . 40
Using the CLI to install firmware . . . 40
One-step firmware installation . . . 40
Custom firmware installation . . . 41
Adding a switch to an existing fabric . . . 42
Installing feature license keys . . . 42
Configuring Call Home to HP Services (optional) . . . 42
Role of the Remote Support Software Manager . . . 43
Role of OSEM and versions required . . . 43
Installation instructions and documentation for SIM, RSP, and OSEM . . . 43
RSP requirements for the CMS . . . 43
Infrastructure requirements for implementing Call Home to HP Services . . . 44
Configuring Call Home to HP services . . . 44

4 Diagnostics and Troubleshooting . . . 47
Switch diagnostics . . . 47
Input power LED is extinguished . . . 47
System fault LED is illuminated . . . 47
Power-On self test diagnostics . . . 48
Heartbeat LED blink patterns . . . 48
Internal firmware failure blink pattern . . . 48
Fatal POST error blink pattern . . . 48
Configuration file system error blink pattern . . . 49
Over-temperature blink pattern . . . 49
Logged-in LED indications . . . 50
E_Port isolation . . . 50
Excessive port errors . . . 51
Transceiver diagnostics . . . 52
Recovering a switch using maintenance mode . . . 53
Exiting the maintenance menu (option 0) . . . 53
Unpacking a firmware image file in maintenance mode (option 1) . . . 54
Resetting the network configuration in maintenance mode (option 2) . . . 54
Resetting user accounts in maintenance mode (option 3) . . . 54
Copying log files in maintenance mode (option 4) . . . 54
Removing the switch configuration in maintenance mode (option 5) . . . 54
Remaking the file system in maintenance mode (option 6) . . . 54
Resetting the switch in maintenance mode (option 7) . . . 55
Updating the boot loader in maintenance mode (option 8) . . . 55

5 Support and Other Resources . . . 57
Document conventions and symbols . . . 57

Contacting HP . . . 58
HP contact information . . . 58
Rack stability . . . 58
Subscription service . . . 58
Documentation feedback . . . 58
New and changed information in this edition . . . 58
Related information . . . 58
Documents . . . 58
Other HP websites . . . 59
Customer self repair . . . 59

A Regulatory Compliance and Safety . . . 61
Regulatory compliance . . . 61
Federal Communications Commission notice for Class A equipment . . . 61
Cables . . . 61
Laser device . . . 61
Laser safety warning . . . 61
Certification and classification information . . . 62
Laser product label . . . 62
International notices and statements . . . 62
Canadian notice (avis Canadien) . . . 62
European Union regulatory notice . . . 63
Japanese notice . . . 63
Korean notice . . . 63
Taiwan notice . . . 63
Chinese warning messages . . . 64
Altitude warning message . . . 64
Non-tropical warning message . . . 64

B How to Prevent Electrostatic Discharge . . . 65
Grounding methods . . . 65

C Technical Specifications . . . 67
General specifications . . . 67
Maintainability features . . . 68
Fabric management specifications . . . 69
Weight and physical dimensions . . . 69
Electrical specifications . . . 69
Environmental requirements . . . 70

D Factory Configuration Defaults . . . 71
Factory switch configuration . . . 71
Factory port configuration . . . 72
Factory port threshold alarm configuration . . . 73
Factory zoning configuration . . . 73
Factory SNMP configuration . . . 74
Factory switch services configuration . . . 74
Factory DNS host name configuration . . . 75
Factory IP version 4 Ethernet configuration . . . 75
Factory IP version 6 Ethernet configuration . . . 75
Factory event logging configuration . . . 76
Factory NTP server configuration . . . 76
Factory timer configuration . . . 76
Factory RADIUS configuration . . . 77
Factory security configuration . . . 77
Factory Call Home configuration . . . 78

Glossary . . . 79

Index . . . 83

Figures

1 8/20q Fibre Channel Switch . . . 7
2 Switch LEDs and controls . . . 8
3 Fibre Channel ports . . . 10
4 Port LEDs . . . 10
5 Ethernet port . . . 12
6 Serial port and pin identification . . . 12
7 Attaching the rails to the switch . . . 33
8 Installing the rear mounting brackets . . . 33
9 Installing the switch and rail assembly . . . 33
10 Fastening the rail to the front of the rack . . . 34
11 Fastening the rail to the rear mounting bracket . . . 34
12 Installing the filler panel . . . 34
13 Management station and workstation cable connections . . . 37
14 Switch LEDs . . . 47
15 Logged-in LED . . . 50
16 Class 1 laser product label . . . 62

Tables

1 Fibre Channel port types . . . 11
2 Serial port pin identification . . . 13
3 Zoning database limits . . . 17
4 Extended credit distances . . . 18
5 Extended credit minimum cable lengths . . . 18
6 Port-to-port latency . . . 19
7 Management station requirements for SAN Connection Manager and Enterprise Fabric Management Suite . . . 29
8 Workstation requirements for QuickTools . . . 29
9 8/20q and SN6000 Fibre Channel Switch rack mount kit hardware . . . 32
10 Document conventions . . . 57
11 General specifications for the 8/20q Fibre Channel Switch . . . 67
12 Maintainability feature for the 8/20q Fibre Channel Switch . . . 68
13 Fabric management specifications for the 8/20q Fibre Channel Switch . . . 69
14 Switch physical dimensions for the 8/20q Fibre Channel Switch . . . 69
15 Electrical specifications for the 8/20q Fibre Channel Switch . . . 69
16 Environmental requirements . . . 70
17 Switch configuration defaults . . . 71
18 Port configuration defaults . . . 72
19 Port threshold alarm configuration defaults . . . 73
20 Zoning configuration defaults . . . 73
21 SNMP configuration defaults . . . 74
22 Services configuration defaults . . . 74
23 DNS host name configuration defaults . . . 75
24 IP version 4 Ethernet configuration defaults . . . 75
25 IP version 6 Ethernet configuration defaults . . . 75
26 Event logging configuration defaults . . . 76
27 NTP server configuration defaults . . . 76
28 Timer configuration defaults . . . 76
29 RADIUS configuration defaults . . . 77
30 Security configuration defaults . . . 77
31 Call Home service configuration defaults . . . 78

1 General Description

The HP 8/20q Fibre Channel Switch (Figure 1) is a 20-port, 8-Gb/s switch with both Ethernet and serial management interfaces. This chapter describes the features and capabilities of the HP 8/20q Fibre Channel Switch.

You can manage fabrics with the Command Line Interface (CLI), the QuickTools web applet, or the optional Enterprise Fabric Management Suite. You can also use the HP SAN Connection Manager, which provides basic switch management functions, such as IP address configuration, and limited control of zoning.

- For more information about the CLI, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.
- For information about QuickTools, see the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*.
- For information about SAN Connection Manager, see the *HP SAN Connection Manager User Guide*.
- For information about downloading Enterprise Fabric Management Suite with a 30-day trial license, see the HP website www.hp.com/go/EFMS.

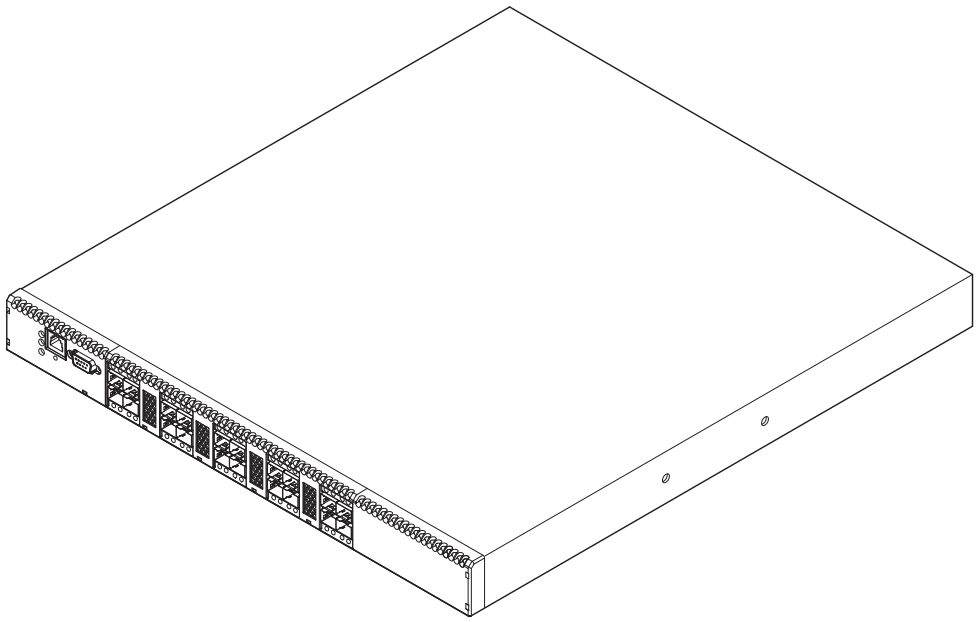
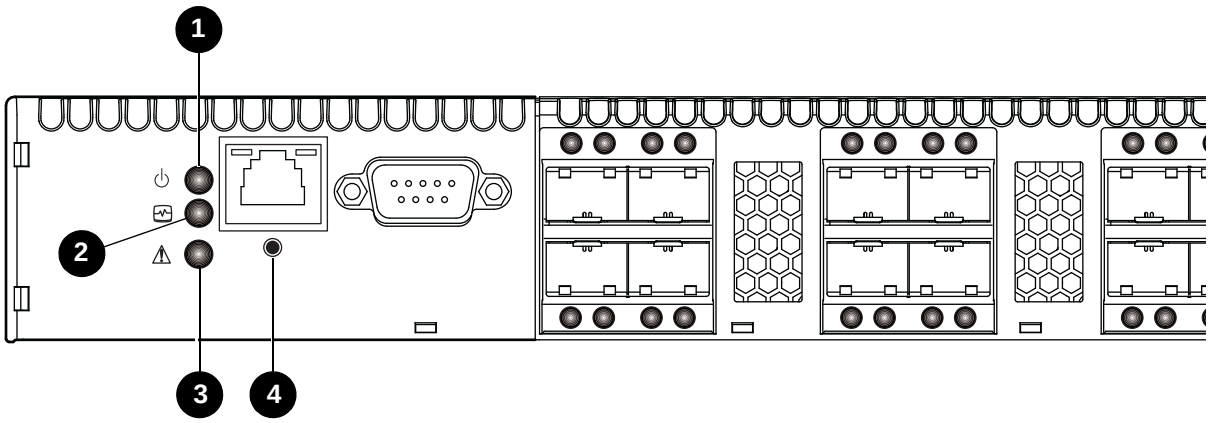


Figure 1 8/20q Fibre Channel Switch

Switch LEDs and controls

The switch LEDs provide information about the switch's operational status. These LEDS include the Input Power LED (green), Heartbeat LED (green), and the System Fault LED (amber) (Figure 2). For information about port LEDs, see "Port LEDs" (page 10). The Maintenance button (Figure 2) is the only switch control. It is used to reset a switch or to recover a disabled switch. To apply power to the switch, plug the power cord into the switch AC power receptacle, located on the back of the switch, and into a 100–240 VAC power source.



1 Input Power LED (green)
2 Heartbeat LED (green)
3 System Fault LED (amber)
4 Maintenance button

Figure 2 Switch LEDs and controls

Input power LED (green)

The Input Power LED indicates the voltage status at the switch logic circuitry. During normal operation, this LED illuminates to indicate that the switch logic circuitry is receiving the proper DC voltages. When the switch is in maintenance mode, this LED is extinguished.

Heartbeat LED (green)

The Heartbeat LED indicates the status of the internal switch processor and the results of the POST. Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. For more information, see "Heartbeat LED blink patterns" (page 48).

System fault LED (amber)

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. Fault conditions include POST errors, over-temperature conditions, and power supply malfunctions. The Heartbeat LED shows a blink code for POST errors and over-temperature conditions. For more information, see "Heartbeat LED blink patterns" (page 48).

Maintenance button

The Maintenance button (Figure 2) is a dual-function momentary switch on the front panel. Its purpose is to reset the switch or to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. For more information, see "Recovering a switch using maintenance mode" (page 53).

Resetting a switch

To reset the switch, press and hold the Maintenance button with a pointed tool for less than two seconds. The switch responds as follows:

- All the switch LEDs illuminate except the System Fault LED.
- After approximately one minute, the power-on self test (POST) begins, extinguishing the Heartbeat LED.
- When the POST finishes, the Input Power LED illuminates and the Heartbeat LED flashes once per second.

Placing the switch in maintenance mode

To place the switch in maintenance mode:

1. Isolate the switch from the fabric.
2. Press and hold the Maintenance button with a pointed tool for a few seconds until only the Heartbeat LED (Figure 2) is illuminated. Continue holding the maintenance button until the Heartbeat LED goes off, then release the button. The Heartbeat LED illuminates continuously while the switch is in maintenance mode.

To exit maintenance mode and return to normal operation, press and release the Maintenance button momentarily to reset the switch.

Fibre Channel ports

The 8/20q Fibre Channel Switch has twenty Fibre Channel ports. Ports are numbered 0–19 (Figure 3). Each of the ports is served by a Small Form-Factor Pluggable (SFP+) transceiver and is capable of 8-Gb/s, 4-Gb/s, or 2-Gb/s transmission.

- SFPs are hot-pluggable.
- User ports can self-discover both the port type and transmission speed when connected to devices or other switches.
- The port LEDs are located above ports 0–9 and below ports 10–19, and provide port login and activity status information.

NOTE: Setting a Fibre Channel port that has an 8-Gb/s SFP transceiver to 1-Gb/s will down the port.

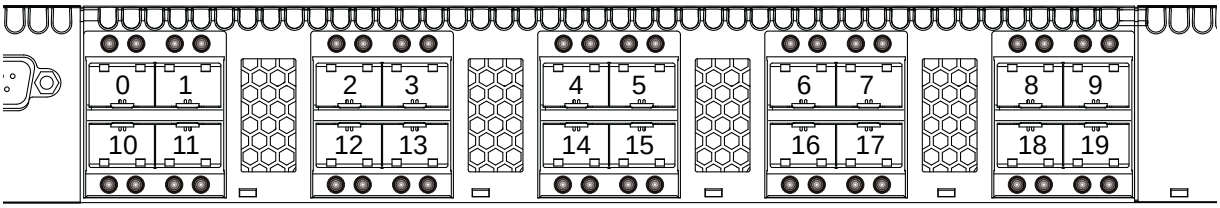
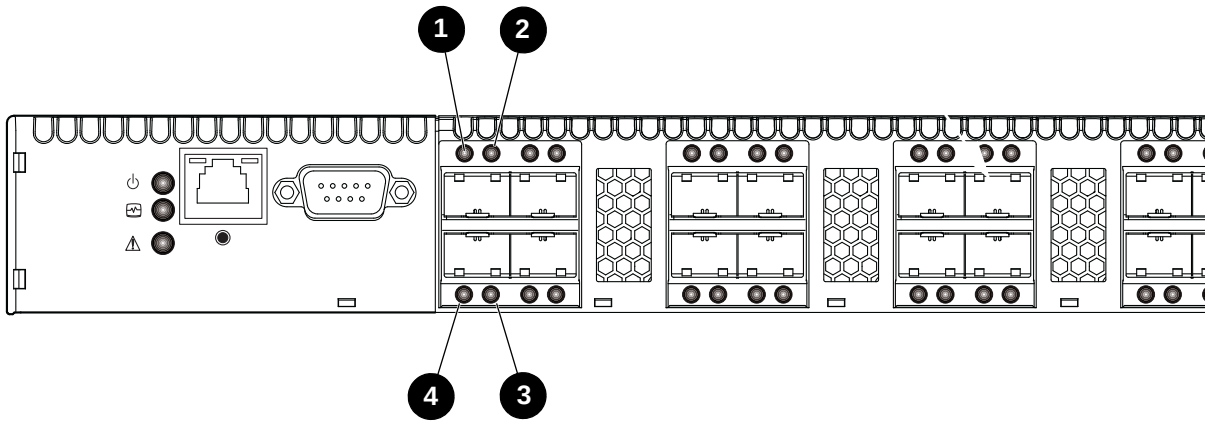


Figure 3 Fibre Channel ports

The 8/20q Fibre Channel Switch comes from the factory as an 8- or 16-port switch, enabling ports 0–7 or 0–15 respectively. You can enable additional ports up to the 20-port maximum using the HP 8/20q 4-port Upgrade License. For more information, see "Installing feature license keys" (page 42).

Port LEDs

Each port has its own Logged-in LED (green) and Activity LED (green) (Figure 4).



1 Logged-in LED (port 0)
2 Activity LED (port 0)
3 Activity LED (port 10)
4 Logged-in LED (port 10)

Figure 4 Port LEDs

Port Logged-in LED (green)

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-in LEDs. Following a successful port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-in LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-in LED is extinguished. For more information, see "Logged-in LED indications" (page 50).

Port Activity LED (green)

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives illuminates this LED for 50 milliseconds. This makes it possible to observe the transmission of a single frame.

Transceivers

The 8/20q Fibre Channel Switch supports SFP+ optical transceivers for the Fibre Channel ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fiber optic cables plug into the transceivers which then connect to the devices. A port is capable of transmitting at 8 Gb/s, 4 Gb/s, or 2 Gb/s; however, the transceiver must also be capable of delivering at this rate.

The SFP+ transceivers are hot-pluggable. This means that you can remove or install a transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. For information about installing and removing SFP+ optical transceivers, see "Install the transceivers" (page 35).

Port types

The 8/20q Fibre Channel Switch supports generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), expansion ports (E_Port), and transparent routing ports (TR_Port). Switches come from the factory with all Fibre Channel ports configured as GL_Ports. Table 1 describes generic, fabric, expansion, and transparent routing port functions.

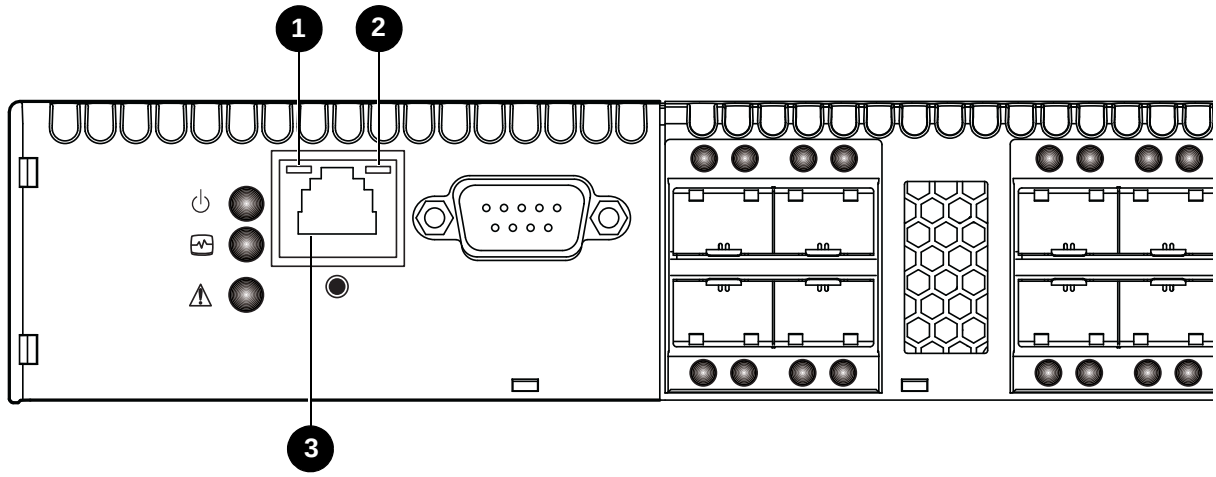
Table 1 Fibre Channel port types

Port type	Description
GL_Port	Generic loop port—self-configures as an FL_Port when connected to a loop device, as an F_Port when connected to a single device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
G_Port	Generic port—self-configures as an F_Port when connected to a single device, or as an E_Port when connected to another switch.
FL_Port	Fabric loop port—supports a loop of up to 126 devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single device (N_Port).
F_Port	Fabric port—supports a single device.
E_Port	Expansion port—expands the fabric by connecting 8/20q Fibre Channel Switches. The 8/20q Fibre Channel Switch self-discovers all inter-switch connections. For more information, see "Multiple switch fabrics" (page 20).
TR_Port	Transparent routing port—expands the fabric by connecting an 8/20q Fibre Channel Switch to an HP B-series or C-series remote fabric. The TR_Port provides transparent communication between local fabric devices and remote fabric devices while maintaining separate fabrics. For more information, see "Transparent routing" (page 21).

Ethernet port

The Ethernet port is an RJ-45 connector that provides a connection to a workstation through a 10/100 Base-T Ethernet cable (Figure 5). A workstation can be a Windows or a Linux server that is used to configure and manage the switch fabric. An Ethernet connection to the switch is required to manage the switch using the CLI, QuickTools, Enterprise Fabric Management Suite, SAN Connection Manager, or Simple Network Management Protocol (SNMP).

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (green). The Link Status LED illuminates continuously when an Ethernet connection has been established. The Activity LED illuminates when data is being transmitted or received over the Ethernet connection.

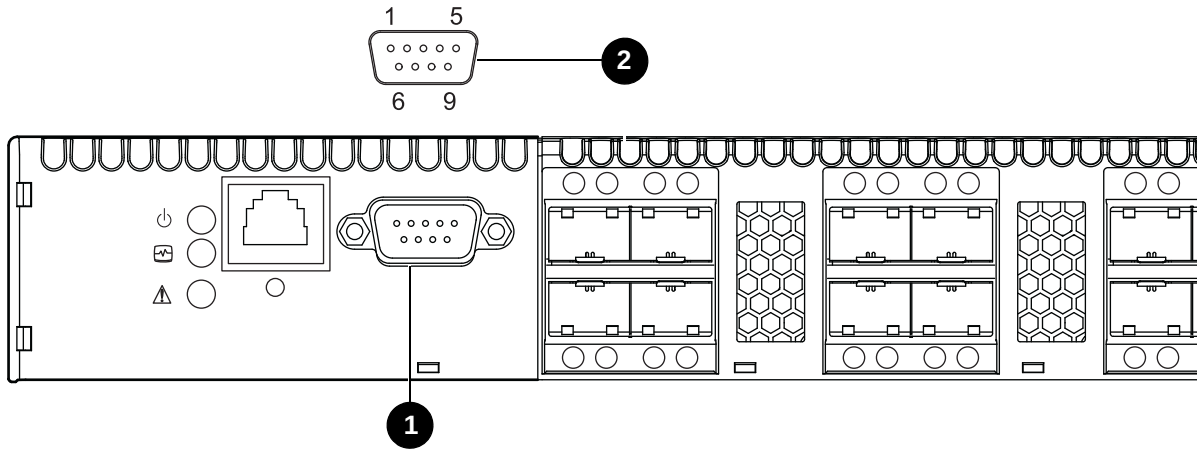


1 Activity LED
2 Link status LED
3 RJ-45 Ethernet port

Figure 5 Ethernet port

Serial port

The 8/20q Fibre Channel Switch is equipped with an RS-232 serial port for maintenance purposes (Figure 6). You can manage the switch through the serial port using the CLI.



1 Serial port
2 RS-232 connector pin identification

Figure 6 Serial port and pin identification

The serial port connector requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector (Figure 6) are identified in Table 2. For information about connecting the workstation through the serial port, see "Connect the management station or workstation to the switch" (page 37).

Table 2 Serial port pin identification

Pin Number	Description	Referred to as
1	Carrier Detect	DCD
2	Receive Data	RxD
3	Transmit Data (TxD)	TxD
4	Data Terminal Ready (DTR)	DTR
5	Signal Ground (GND)	GND
6	Data Set Ready (DSR)	DSR
7	Request to Send (RTS)	RTS
8	Clear to Send (CTS)	CTS
9	Ring Indicator (RI)	RI

Power supply and fans

The switch has a single power supply that converts 100–240 VAC to DC voltages for the various switch circuits. Four internal fans provide cooling. The switch monitors internal air temperature, and therefore does not monitor or report fan operational status. Air flow is front-to-back. To energize the switch, plug the power cord into the switch AC receptacle (located on the back of the switch) and into a 100–240 VAC power source.

Switch management

The switch supports the following management tools and protocols:

- QuickTools web applet, page 14
- SAN Connection Manager, page 14
- Command line interface, page 14
- Enterprise Fabric Management Suite, page 14
- Simple Network Management Protocol, page 14
- Storage Management Initiative–Specification (SMI-S), page 15
- File transfer protocols, page 15

QuickTools web applet

QuickTools is a browser-based graphical user interface (GUI) that provides switch management capabilities beyond those of SAN Connection Manager. You run QuickTools by opening the switch IP address with an internet browser on your workstation. See the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*. QuickTools provides the following management features:

- Faceplate device management
- Switch and port statistics
- Configuration wizard
- Zoning administration
- Fabric tree for fabric management
- User account configuration
- Switch and fabric events
- Operational and environmental statistics
- Global device nicknames
- Inband management of other switches in the fabric
- Online help

SAN Connection Manager

HP SAN Connection Manager is a GUI-based management application for HP that runs on a workstation known as the management station. It provides basic automated configuration and management of switches, HBAs, and storage devices.

Command line interface

The command line interface (CLI) provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. For more information, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

Enterprise Fabric Management Suite

Enterprise Fabric Management Suite is a separately licensed, workstation-based fabric management GUI that includes the capabilities of the QuickTools web applet plus:

- Fabric tracker for monitoring firmware versions
- Port threshold alarm configuration
- Performance view for port performance monitoring
- Extended credits wizard
- mPort technology for moveable port licenses
- Media diagnostics
- Fibre Channel tracing and connection verification

Enterprise Fabric Management Suite can be downloaded with a 30-day trial license from the HP website: www.hp.com/go/EFMS. For information about configuring the switch using Enterprise Fabric Management Suite, see the *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*.

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. The switch firmware supports SNMP versions 1, 2, and 3, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2. SNMP version 3 provides secure access to devices through a combination of authentication and encryption. You can enable SNMP, configure SNMP traps, and configure SNMP version 3 security using the command line interface, QuickTools, or Enterprise Fabric Management Suite.

Storage Management Initiative–Specification (SMI-S)

SMI-S provides for the management of the switch through third-party applications that use the SMI-S. For more information, see the *HP 8/20q and SN6000 Fibre Channel Switch CIM Agent Reference Guide*.

File transfer protocols

FTP and TFTP provide the command line interface for exchanging files between the switch and the workstation. These files include firmware image files, configuration files, and log files. For more information about FTP and TFTP, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

2 Planning a Fabric

This chapter contains information about planning a fabric.

Devices

When planning a fabric, consider the following:

- The number of devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches.
- The transmission speeds of your HBAs and SFPs. The switch supports 2-Gb/s, 4-Gb/s and 8-Gb/s transmission speeds.

> **IMPORTANT:** Setting a Fibre Channel port that has an 8-Gb/s SFP transceiver to 1-Gb/s will down the port.

- The distribution of targets and initiators. An F_Port supports a single device. An FL_Port can support up to 126 devices in an arbitrated loop.

Device access

Consider device access needs within the fabric. Access is controlled by the use of zoning. Some zoning strategies include the following:

- Separating devices by operating system
- Separating devices that have no need to communicate with other devices in the fabric or have classified data
- Separating devices into department, administrative, or other functional group

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. Zoning is hardware-enforced only when a port/device is a member of no more than eight zones whose combined membership does not exceed 64. If this condition is not satisfied, that port behaves as a soft zone member. You can assign ports/devices to a zone individually or as a group by creating an alias.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch. Table 3 describes the zoning database limits, excluding the active zone set.

Table 3 Zoning database limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256).
MaxZones	Maximum number of zones (2,000).
MaxAliases	Maximum number of aliases (2,500).
MaxTotalMembers	Maximum number of zone and alias members (10,000) that can be stored in the zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2,000), excluding the orphan zone set. Each instance of a zone in a zone set counts toward this maximum.

Table 3 Zoning database limits (Continued)

Limit	Description
MaxMembersPerZone	Maximum number of members in a zone (2,000).
MaxMembersPerAlias	Maximum number of members in an alias (2,000)

Performance

The 8/20q Fibre Channel Switch supports class 2 and class 3 Fibre Channel service at transmission rates of 8-Gb/s with a maximum frame size of 2,148 bytes. Related performance characteristics include the following:

- Distance, page 18
- Bandwidth, page 19
- Latency, page 19

Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. For more information about cable types and transceivers, see "Technical Specifications" (page 67).

Each Fibre Channel port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fibre optic cables, this enables full bandwidth over approximately 3 kilometers at 8 Gb/s (4.8 credits/km).

With the optional Enterprise Fabric Management Suite application, longer distances can be spanned at full bandwidth on SFP ports by extending credits to G_Ports, F_Ports, and E_Ports. Each port can donate 15 credits to a pool from which a recipient port can borrow. The recipient port also loses a credit in the process. For example, you can configure an SFP recipient port to borrow 15 credits from one donor port for a total of 30 credits (15+15=30). For more information about Enterprise Fabric Management Suite, see "Enterprise Fabric Management Suite" (page 14).

Table 4 describes the possible distances for a port with 30 credits as an example.

Table 4 Extended credit distances

Transmission Speed	Range for 30 Credits
1 Gb/s	50 kilometers (30÷0.6)
2 Gb/s	25 kilometers (30÷1.2)
4 Gb/s	12 kilometers (30÷2.4)
8 Gb/s	6 kilometers (30÷4.8)

Extending credits requires a minimum cable length that is dependent on transmission speed, but is independent of the number of credits borrowed. Extending credits using short cables can cause excessive port resets. Table 5 describes the minimum cable lengths for a port with extended credits.

Table 5 Extended credit minimum cable lengths

Transmission Speed	Minimum Cable Length
1 Gb/s	3 kilometers
2 Gb/s	1.5 kilometers
4 Gb/s	0.75 kilometers
8 Gb/s	0.37 kilometers

For more information about cable types, transceivers, and maximum supported distances, see the SAN Design Reference Guide available at the HP website: http://www.hp.com/go/SANdesignguide.

Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A Fibre Channel port can transmit or receive at nominal rates of 8 Gb/s, 4 Gb/s, or 2 Gb/s depending on the device to which it is connected. This corresponds to full duplex bandwidth values of 1,700 MB, 850 MB, and 424 MB respectively. Multiple source ports can transmit to the same destination port if the destination bandwidth is greater than or equal to the combined source bandwidth. For example, two 4 Gb/s source ports can transmit to one 8 Gb/s destination port. Similarly, one source port can feed multiple destination ports if the combined destination bandwidth is greater than or equal to the source bandwidth.

In multiple switch fabrics, each link contributes up to 1,700 MB of bandwidth between those switches, depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order delivery with any number of links.

Latency

Latency is a measure of how fast a frame travels through a switch from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship (Table 6).

Table 6 Port-to-port latency

	Destination Rate			
Source Rate	**Gbps**	**2**	**4**	**8**
	2	< 0.6 µsec	< 0.7 µsec[1]	< 0.6 µsec[1]
	4	< 0.4 µsec	< 0.3 µsec	< 0.4 µsec[1]
	8	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec

1 Based on minimum frame size of 36 bytes. Latency increases for larger frame sizes.

Feature licenses

License keys provide a way to expand the capabilities of your switch and fabric as your needs grow. The HP 8/20q 4-port Upgrade License activates additional Fibre Channel ports to 12, 16, or 20 ports. Applying a license key is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller. For more information, see "Installing feature license keys" (page 42). The following license key feature is available:

- The HP 8/20q 4-port Upgrade License enables additional SFP ports to12, 16, or 20 ports.

Multiple switch fabrics

By connecting switches to one another, you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric can automatically resolve domain ID conflicts. Because the Fibre Channel ports are self-configuring, you can connect 8/20q Fibre Channel Switches together in a wide variety of topologies. When planning your fabric, consider your topology and cabling requirements. Transparent routing to a legacy fabric is also possible using TR_Ports.

For more information about Storage Area Network (SAN) connectivity, see the *SAN Design Reference Guide* available at the HP website: http://www.hp.com/go/SANdesignguide.

Optimizing device performance

When choosing a topology for a multiple switch fabric, you should also consider the proximity of your server and storage devices and the performance requirements of your application. Storage applications such as video distribution, medical record storage/retrieval, or real-time data acquisition can have specific latency or bandwidth requirements.

The 8/20q Fibre Channel Switch provides the lowest latency of any product in its class. For information about latency, see "Performance" (page 18). However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance, place devices on the same switch under the following conditions:

- Heavy I/O traffic between specific server and storage devices.
- Distinct speed mismatch between devices such as the following:
  - An 8-Gb/s server and a slower 4-Gb/s storage device
  - A high performance server and slow tape storage device

Domain ID, principal priority, and domain ID lock

The following switch configuration settings affect multiple switch fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1–239 that identifies each switch in a fabric. The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest Worldwide Name (WWN) becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. For information about changing the default domain ID, domain ID lock, and principal priority parameters, see the `set config switch` command in the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. You can remedy this by resetting the new switch or taking it offline then putting it back online. The principal switch will reassign the domain ID and the switch will join the fabric.

NOTE: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs. Domain ID reassignment has no effect on zone members defined by WWN.

Common topologies

For additional information about Storage Area Network (SAN) connectivity, see the *SAN design reference guide* available at the HP website: http://www.hp.com/go/SANdesignguide.

Transparent routing

IMPORTANT: The SAN Connection Manager (SCM) application version 2.10 or later can manage 8/20q Fibre Channel Switches with active TR_Ports; however, SCM cannot manage or discover remote switches or devices in the remote fabric. Use QuickTools or Enterprise Fabric Management Suite and the storage management interface to present Logical Unit Numbers (LUNs) to remote devices. SCM version 2.0 and earlier versions do not support the management of fabrics that include 8/20q Fibre Channel Switches with active TR_Ports and may disrupt communication between the 8/20q Fibre Channel Switch and the remote fabric.

The transparent routing feature provides inter-fabric routing to allow controlled and limited access between devices on a 8/20q Fibre Channel Switch (local) fabric and devices on a remote fabric consisting of B-series or C-series switches. For a list of switches that are supported in a remote fabric, see the *HP 8/20q Fibre Channel Switch release notes*, and the *HP SAN Design reference guide* located at the HP website: http://www.hp.com/go/sandesignguide. This type of inter-fabric connection uses the Fibre Channel industry N-Port ID Virtualization (NPIV), and makes local and remote devices accessible to each other while maintaining the local and remote fabrics as separate fabrics.

You can connect multiple 8/20q Fibre Channel Switches to one or more remote fabrics using multiple TR_Ports. Local and remote devices are identified by their respective port worldwide names. Consider the following mapping rules:

- A TR_Port can support a maximum of 32 local device/remote device mappings.
- A specific local device can be mapped to devices on only one remote fabric. Local devices on the same 8/20q Fibre Channel Switch can each be mapped to different remote fabrics.
- For mappings between a specific 8/20q Fibre Channel Switch and a remote fabric, each local device or remote device can be mapped over only one TR_Port. Additional mappings to either device must use that same TR_Port.
- Mulitple local devices connected to different local switches can be mapped to the same remote device over one TR_Port on each local switch.
- A local device cannot be mapped over an E_Port to another local switch, then over a TR_Port to the remote device. The local switch to which the local device is connected must connect directly to the remote fabric over a TR_Port.

NOTE: When a local device is mapped over a TR_Port to a remote device, the local device and its TR_Port appear as an NPIV connected device in the remote fabric. It is possible, though not recommended, to map such a local device over a second TR_Port to a local device in a second local fabric. In this case, if you merge the two local fabrics, the transparent route becomes inactive for the devices that now have a path over an ISL, and an alarm is generated.

You can configure transparent routing using QuickTools, Enterprise Fabric Management Suite, or the CLI, though QuickTools and Enterprise Fabric Management Suite are recommended because they validate your entries, manage the zone mapping for the local fabric, and create a list of zoning commands that can be run in a script on a HP B-series or C-series SAN switch. For more information, see the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*, *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*, or the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

IMPORTANT: Since C-series switches do not support the Unzoned Name Server, C-series fabrics must be "pre-zoned" before you can set up TR mappings to a remote C-series fabric using the TR Mapping Manager dialog box. The C-series fabric zoneset must be changed to add zones so that the WWNs of the remote devices are mapped and the WWNs of the 8/20q Fibre Channel Switch TR ports are zoned together. For more information, see the C-series documentation for specific information to configure zoning. Retain these zones in the zoneset after completion of the TR mapping, until you no longer need to map the device to the local fabric.

To configure transparent routing using QuickTools or Enterprise Fabric Management Suite:

1. Determine what devices on the local fabric require access to devices on the remote fabric. Local devices must be attached directly to the 8/20q Fibre Channel Switch.
2. Configure one or more TR_Ports on the local 8/20q Fibre Channel Switch, and then connect the TR_Port to the remote fabric. The application prompts you to configure TR_Ports where existing port connections to remote fabrics are isolated. For remote HP B-series or C-series fabrics, the switch to which the TR_Port connects must support N-Port ID Virtualization (NPIV) and for B-series fabrics, the interoperability mode must be configured to InteropMode=0. Other B-series or C-series switches in the remote fabric need not support NPIV.

NOTE: Be sure to configure the TR_Port before connecting the remote fabric to the HP 8/20q Fibre Channel Switch. If the remote fabric is connected to a port on the HP 8/20q Fibre Channel Switch that is not a TR_Port, the two fabrics may establish an E_Port connection and the local and remote fabrics may merge. This mixed fabric is not supported . If the port type is changed to TR_Port after connecting the remote fabric, a port reset may be required to completely establish the connection.

3. Map local devices to remote devices and activate the connection. The mapping process creates an inter-fabric zone (IFZ) in the active zoneset consisting of the local device, the remote device, and the TR_Port. When the mapping is complete, the new zoneset is activated.

   The name of the inter-fabric zone begins with IFZ followed by the lowest device port WWN followed by the remaining port WWN, all uppercase, separated by underscores (_). For example, consider the following local and remote device WWNs:

   - Local device: 21:00:00:e0:8b:0e:d3:59
   - Remote device: 22:00:00:04:cf:a8:7f:2d

   The inter-fabric zone name would be:

   ```
   IFZ_210000E08B0ED359_22000004CFA87F2D
   ```

4. Apply the same inter-fabric zone that was created on the local fabric to the active zoning on the remote fabric. The application creates a suggested list of commands during the mapping process that, when run on a remote fabric consisting of HP B-series or C-series switches, will make the necessary zoning changes to the remote fabric. See the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide* or the *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide* for important details on creating and using this list of suggested commands. When modifications to the active zoning on both fabrics are complete, the transparent routing connection becomes active, and the local devices will discover the remote devices.

Switch services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. Familiarize yourself with the following switch services and determine which ones you need.

- **Telnet:** Provides for the management of the switch over a Telnet connection. Disabling this service is not recommended. The default is `enabled`.
- **Secure Shell (SSH):** Provides for secure remote connections to the switch using SSH. Your workstation must also use an SSH client. The default is `disabled`.
- **GUI Management:** Provides for out-of-band management of the switch with SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, SNMP, and SMI-S. If this service is **disabled, the switch can only be managed inband or through the serial port. The default is enabled.**
- **Inband Management:** Provides for the management of the switch over an inter-switch link using SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, SNMP, or management server. If you disable inband management, you can no longer communicate with that switch by means other than an Ethernet or serial connection. The default is `enabled`.
- **Secure Socket Layer (SSL):** Provides for secure SSL connections for the QuickTools web applet, Enterprise Fabric Management Suite and SMI-S. This service must be enabled to authenticate users through a Remote Authentication Dial-in Service (RADIUS) server. To enable secure SSL connections, you must first synchronize the date and time on the switch and the workstation. Enabling SSL automatically creates a security certificate on the switch. The default is `disabled`.
- **QuickTools web applet (EmbeddedGUI):** Provides for access to the QuickTools web applet. QuickTools enables you to point at a switch with an internet browser and manage the switch through the browser. The default is `enabled`.
- **Simple Network Management Protocol (SNMP):** Provides for the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to these well-known defaults and should be changed if SNMP is to be enabled. Otherwise, you risk unwanted access to the switch. The switch supports SNMP versions 1, 2, and 3. The default configuration enables SNMP and disables SNMP version 3 security.
- **Common Information Model (CIM):** Provides for the management of the switch through third-party applications that use the Storage Management Initiative–Specification (SMI-S). The default is `enabled`.
- **File Transfer Protocol (FTP):** Provides for transferring files rapidly between the workstation and the switch using FTP. The default is `enabled`.

- **Management Server (MS):** Enables or disables the management of the switch through third-party applications that use FC-GS-3 Management Server. The default is `disabled`.
- **Call Home:** If enabled and configured, switches can send alerts regarding events and faults to Email addresses. Users can configure the type of events and where the alerts are sent.

IMPORTANT: The Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies only HP services.

Provides for automated e-mail notification of switch status and operating conditions based on specified event severity levels. The default is `enabled`. The Call Home service requires an Ethernet connection to at least one Simple Mail Transfer Protocol (SMTP) server. You must configure the Call Home service to do the following:

- Enable primary and secondary SMTP servers and specify their IP addresses
- Specify contact information

Configure one or more Call Home profiles to specify e-mail recipients, message format, and the event severity level that will initiate a message. In addition, you can configure periodic event data collection and processing through the Tech_Support_Center profile for automated status and trend analysis.

Security

Security is available at the following levels:

- User account security, page 25
- IP security, page 25
- Port binding, page 26
- Connection security, page 26
- Device security, page 26

User account security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in the CLI, QuickTools, Enterprise Fabric Management Suite, and SAN Connection Manager. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can create or add account names and change passwords of other accounts. All users can change their own passwords. Account names and passwords are always required when connecting to a switch.

Authentication of the user account and password can be performed locally using the switch's user account database or it can be done remotely using a RADIUS server such as Microsoft RADIUS. Authenticating user logins on a RADIUS server requires a secure management connection to the switch. For information about securing the management connection, see "Connection security" (page 26). A RADIUS server can also be used to authenticate devices and other switches as described in "Device security" (page 26).

Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates. Also consider the advantages of centralizing user administration and authentication on a RADIUS server. Use the CLI to configure RADIUS servers. For more information about RADIUS server configuration, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

NOTE: If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

IP security

IP security provides encryption-based security for IPv4 and IPv6 communications through policies and associations. Policies define security for host-to-host and host-to-gateway connections; one policy for each direction. For example, to secure the connection between two hosts, you need two policies: one for outbound traffic from the source to the destination, and another for inbound traffic to the source from the destination. A security association defines the encryption algorithm and encryption key (public key or secret) to apply when called by a security policy. A security policy can call several associations at different times, but each association is related to only one policy.

You must configure matching security associations on the switch and on the connected devices (peers) that require secure IP communication. To simplify the IP security configuration process, the switch supports the Internet key exchange (IKE). IKE is a protocol that automates the configuration of matching IP security associations on the switch and on the connected device (or peer). The IKE peer defines the IKE security association connection through which the IKE policy configures the IP security associations.The IKE policy defines the type of data traffic to secure between the switch and the peer, and how to encrypt that data. You must create the same IKE peer and IKE policy configurations on the switch and the peer device.

Public key encryption requires a public key, a corresponding private key, and the necessary certificates to authenticate them. Public key infrastructure (PKI) provides support for the creation and management of public/private key pairs, signed certificates, and certificate authority (CA) certificates when using IKE. You can create a public/private key and combine it with one or more device identities to generate a certificate request. Submit the certificate request to a CA to obtain a signed certificate, which contains the authenticated public/private key pair. In addition to the signed certificate, you must also obtain a CA certificate to authenticate the CA. After downloading the signed certificate and a CA certificate to the switch and importing them into the PKI database, the signed certificate (which contains the authenticated public key) can then be used to complete the IKE peer configuration.

Consider your IP security requirements and the type of encryption you want to use (public key or secret). Also consider which of the connected devices support IKE, and how you will configure IP security on both the switch and connected devices.

Port binding

Port binding provides authorization for a list of up to 32 switch and device WWNs that are permitted to log in to a particular switch port. Switches or devices that are not among the 32 are refused access to the port. Consider what ports to secure and the set of switches and devices that are permitted to log in to those ports. Use the CLI to configure port binding. For more information about port binding configuration, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

Connection security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as QuickTools, Enterprise Fabric Management Suite, and SMI-S. Use the CLI to configure SSH and SSL. For more information about SSH and SSL configuration, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. When the SSL service is enabled, a certificate is automatically created on the switch. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. The switch certificate is valid 24 hours before its creation date and 365 days after its creation date. If the certificate should become invalid, create a new certificate using the `create certificate` CLI command. For information about the `create certificate` CLI command, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

NOTE: SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of SAN Connection Manager.

Consider your requirements for connection security: for the command line interface (SSH), management applications (SSL), or both. If an SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

Device security

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. Use the CLI to configure device security. For more information about device security configuration, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).

A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 16.
- Maximum number of members in a group is 1,000.
- Maximum total number of group members is 1,000.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a RADIUS server such as Microsoft RADIUS. With a RADIUS server,

the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts as described in "User account security" (page 25). A secure connection is required to authenticate user logins with a RADIUS server. For more information, see "Connection security" (page 26).

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to be distributed on the switches or centralized on a RADIUS server and how many servers to configure. Use the CLI to configure RADIUS servers. For more information about RADIUS server configuration, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

Fabric management

The SAN Connection Manager application is a GUI-based management application for HP that runs on the management station. It provides basic automated configuration and management of switches, HBAs, and storage devices. Switch management functions include IP address configuration and limited control of zoning.

The browser-based application, QuickTools, and the CLI reside in the switch firmware and provide for the management of individual switches in a single fabric.

The Enterprise Fabric Management Suite application is an optional, workstation-based fabric management application that provides for the configuration, control, and maintenance of multiple fabrics. For more information about Enterprise Fabric Management Suite, see the "Enterprise Fabric Management Suite" (page 14).

Consider how many fabrics and switches will be managed, how many workstations are needed, and whether the fabrics will be managed with SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, or the CLI.

A switch supports a combined maximum of 19 logins, which are reserved as follows:

- 4 logins or sessions for internal applications, such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SAN Connection Manager inband and out-of-band logins, QuickTools logins, Enterprise Fabric Management Suite logins, and Telnet logins.

Additional logins will be refused.

3 Installation

This chapter describes how to install and configure the switch.

Site requirements

Consider the following items when installing an 8/20q Fibre Channel Switch.

Management Station and Workstation requirements

The management station requirements for SAN Connection Manager and Enterprise Fabric Management Suite are described in Table 7. Workstation requirements for QuickTools are described in Table 8.

Table 7 Management station requirements for SAN Connection Manager and Enterprise Fabric Management Suite

Operating System	• Windows Server 2003 R2 and Windows Storage Server 2003 R2 x64/x86 with SP2. This requires Microsoft hotfix QFE932755 (updated Storport storage driver). The update is available on the Microsoft Web site: http://support.microsoft.com/kb/932755 • Windows Server 2008 x64/x86 with SP2 • Windows Server 2008 x64/x86 R2
Memory	2 GB
Disk Space	• 200 MB of disk space for HP SAN Connection Manager software • 150 MB of disk space for HP Enterprise Fabric Management Suite
Processor	2 GHz or faster
Internet browser	Microsoft Internet Explorer 6.0 or later Netscape Navigator 6.0 and later Firefox 1.5 and later Java Runtime Environment 1.5 or higher
Hardware	RJ-45 Ethernet port Add RS-232 serial port (optional) PCI-e slots for the HP PCI-e FC HBA

Table 8 Workstation requirements for QuickTools

Operating systems	Windows XP SP1/SP2/SP3 Windows 2003 SP2 Windows 2008 SP2 and R2 Red Hat Enterprise Linux 4, 5 SUSE Linux Enterprise Server 9, 10, and 11
Memory	512 MB
Processor	2 GHz or faster

Table 8 Workstation requirements for QuickTools

Internet Browser	Microsoft Internet Explorer 6.0 or later Netscape Navigator 6.0 and later Firefox 1.5 and later Java Runtime Environment 1.4.2 or later[1]
Hardware	RJ-45 Ethernet port

1. You must disable caching of temporary files and applets in Java to prevent conflicts with past or future versions of QuickTools. Furthermore, you may need to disable caching again after upgrading Java.

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

Switch power requirements

Power requirements are 1 Amp at 100 VAC or 0.5 A at 240 VAC.

Environmental conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 0°–40°C (0°–104°F)
- Relative humidity: 15–80%, non-condensing

Installing a switch

Unpack the switch and accessories. The 8/20q Fibre Channel Switch product is shipped with the following components

- One *Read-Me-First* document
- One *End User License Agreement (EULA)*
- *HP 8/20q and SN6000 Fibre Channel Switch Rack-Mount Kit quick start installation instructions*
- *HP 8/20q and SN6000 Fibre Channel Switch quick start installation instructions*
- One HP SAN Connection Manager software CD
- One HP 8/20q Fibre Channel Switch
- One HP 8/20q and SN6000 Fibre Channel Switch Rack-Mount Kit
- One standard power cord
- One HP Power Distribution Unit (PDU) power cable
- One serial cable
- Four adhesive rubber feet

For the latest product information, including firmware, documentation, and supported SAN configurations, visit the following HP web site: http://www.hp.com/go/8Gb-SSC.

Installing a 8/20q Fibre Channel Switch involves the following steps:

1. Mount the switch, page 31
2. Install the transceivers, page 35
3. Configure the workstation, page 35
4. Apply power to the switch, page 36
5. Connect the management station or workstation to the switch, page 37
6. Configure the switch, page 37
7. Cable devices to the switch, page 39

Mount the switch

The switch can be placed on a flat surface and stacked, or mounted in a 19" Electronics Industries Association (EIA) rack. See "Weight and physical dimensions" (page 69) for weight and dimensional specifications. Adhesive rubber feet are provided for surface mounts only. Without the rubber feet, the switch occupies 1U of space in an EIA rack.

The rack mount kit is supported with the following HP custom racks only:

- HP 9000 Series Rack
- HP 10000 Series Rack
- HP 10000 G2 Series Rack

Before you begin

⚠ **WARNING!** To reduce the risk of personal injury or damage to the equipment, ensure that:

- In single-rack installations, stabilizing feet are attached to the rack.
- In multiple-rack installations, racks are coupled together.
- Leveling jacks on the rack are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- Heavy items, such as uninterruptible power supplies and hard drive storage enclosures, are installed near the bottom of the rack.
- Similar components are installed next to each other in the rack. Because devices are of differing depths, this will facilitate maintenance and service tasks.
- Only one device in a rack is extended at a time. A rack may become unstable if more than one device is extended.

△ **CAUTION:**

- For proper airflow, the SFP+ media side (port side) of the device must face the front of the rack. Mounting the switch in this direction allows air to enter from the front of the rack (SFP-port side of switch) and exhaust through the back of the rack (power-supply side of switch). This prevents overheating, which may cause equipment in the rack to fail.
- Allow a minimum of 63.5 cm (25 in.) clearance in front of the rack to allow the doors to open fully, and 76.2 cm (30 in.) in back of the rack to allow for servicing and airflow.
- If the device is mounted in a closed rack or there are multiple rack-mounted devices, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature.
- Multiple rack-mounted devices connected to the same AC supply circuit may overload that circuit or the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit.
- Reliable grounding in the rack must be maintained.

Collect the required items

NOTE: The rack mount kit installation requires one technician.

Locate the following items and set them aside:

- 8/20q Fibre Channel Switch
- 8/20q and SN6000 Fibre Channel Switch rack-mount kit
- Smaller items, such as screws, ship in plastic bags in the kit. See Table 9.

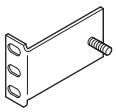
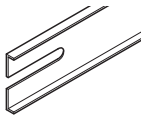
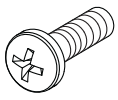
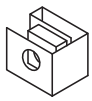
Required tools:

- #2 Phillips screwdriver
- 7/16-inch wrench

Verify the kit contents

Check the contents of the 8/20q and SN6000 Fibre Channel Switch rack mount kit shipping carton to verify that all required parts and hardware are available (Table 9).

Table 9 8/20q and SN6000 Fibre Channel Switch rack mount kit hardware

Item	Description
	Two (2) rear mounting brackets
	Two (2) switch rails
	One (1) filler panel (optional), see step 7.
	Ten (10) M6 machine screws
	Ten (10) M6 cage-nuts for square rack holes
	Ten (10) M6 cage-nuts for round rack holes
	Four (4) 10-32 x .375-inch screws with captive washers
	Two (2) 1/4-20 hex nuts with lock washers
	Two (2) 1/4-inch flat washers

Rack the switch

1. Remove and discard the four 10-32 screws from the sides of the switch.
2. Attach each rail to the switch using two 10-32 x .375-inch screws with captive washers (Figure 7). Make sure the slotted ends of the rails are on the power-supply side (not the SFP-port side) of the switch.

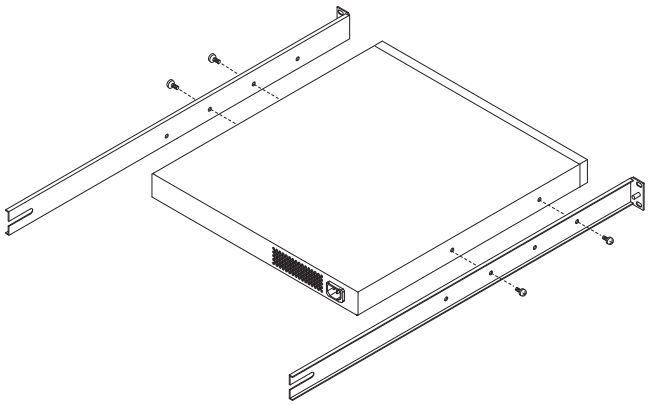


Figure 7 Attaching the rails to the switch

3. On the rack vertical posts, mark the holes that will be used by the rail flanges (three on each rear vertical post, two on each front vertical post). Then, from the inside of each vertical post, insert an M6 cage-nut for the rack you are using (square or round hole) into each marked hole (Figure 8).

   Fasten each rear mounting bracket to the marked holes, using two M6 machine screws.

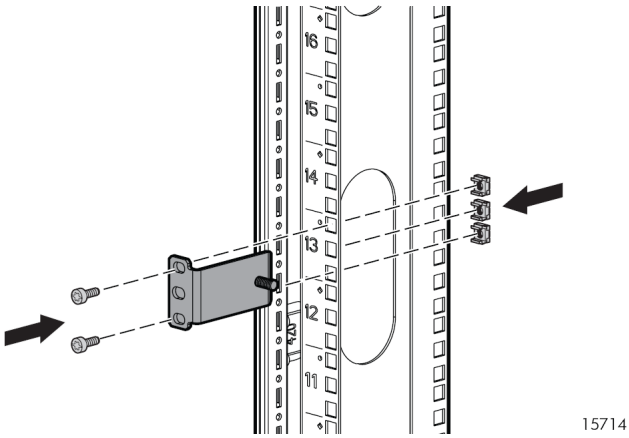


Figure 8 Installing the rear mounting brackets

4. Place the switch and rail assembly into the rack through the front, guiding the slotted-rail ends onto the threaded studs of the rear mounting brackets (Figure 9). Fit the posts on the front rail flanges in the holes between the two cage-nuts on each of the front vertical rack posts.

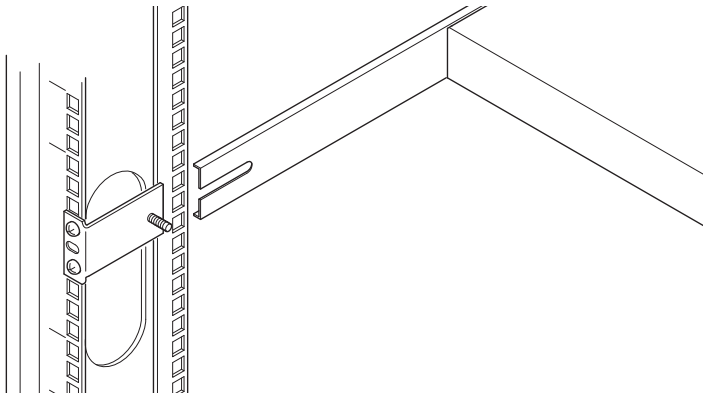


Figure 9 Installing the switch and rail assembly

5. Fasten each rail flange to the front of the rack using two M6 machine screws (Figure 10).

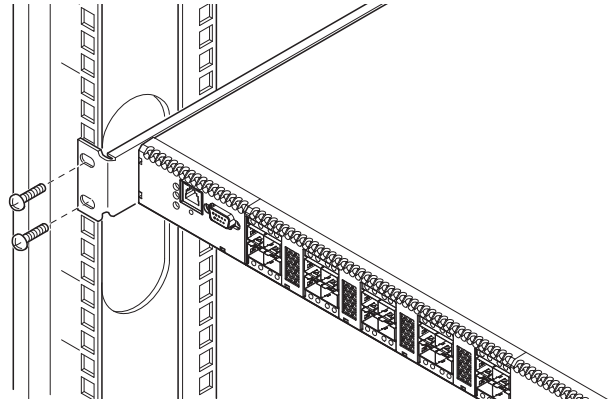


Figure 10 Fastening the rail to the front of the rack

6. Fasten each slotted-rail end to the rear mounting bracket using a flat washer and a 1/4-20 hex nut (Figure 11).

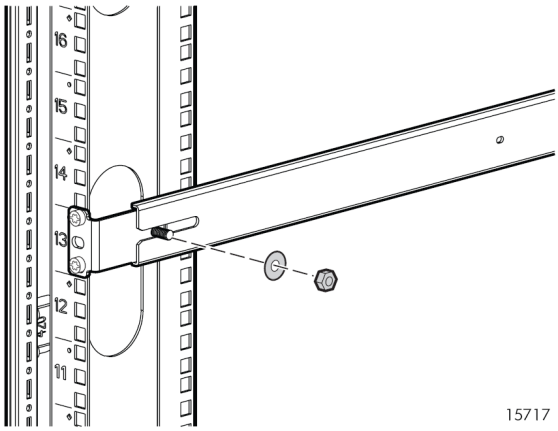


Figure 11 Fastening the rail to the rear mounting bracket

7. Optional: Fasten the filler panel to the rear mounting brackets with two M6 machine screws (Figure 12).

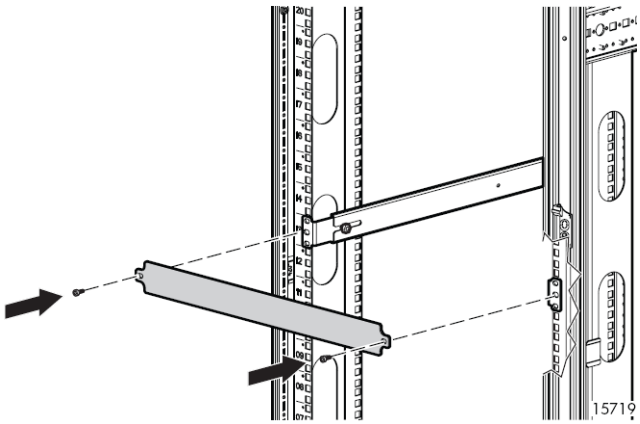


Figure 12 Installing the filler panel

Install the transceivers

A small form-factor pluggable (SFP) transceiver is required for each switch port that will be connected to a device or another switch. SFPs are not included with the switch. Only HP SFPs are supported for use in the switch. To install an SFP transceiver, insert the transceiver into any of the active switch ports and gently press until it snaps in place.

TIP: The transceiver will fit only one way. If the transceiver is not installed under gentle pressure, invert it over and try again.

A new switch has eight (ports 0–7) or sixteen (ports 0–15) active ports depending on the model. Additional ports can be activated with the HP 8/20q 4-port Upgrade License. For more information, see "Installing feature license keys" (page 42).

Configure the workstation

NOTE: If you plan to use SAN Connection Manager, QuickTools, or Enterprise Fabric Management Suite to manage the switch, proceed to "Apply power to the switch" (page 36).

If you plan to use the CLI to configure and manage the switch, you must configure the workstation. This involves setting the workstation IP address for Ethernet connections, or configuring the workstation serial port.

Configuring the workstation IP address for Ethernet connections

The default IP address of a new switch is 10.0.0.1. To ensure that your workstation is configured to communicate with the 10.0.0 subnet:

- For a Windows workstation:
  a. Click **Start**, then choose **Settings > Control Panel > Network and Dial-Up Connections**.
  b. Choose **Make New Connection**.
  c. Click the **Connect to a private network through the Internet** radio button, then click **Next**.
  d. Enter **10.0.0.253** for the IP address.
- For a Linux workstation, open a command window and enter the following command where *interface* is your interface name:

```
ifconfig interface ipaddress 10.0.0.253 netmask 255.255.255.0 up
```

Configuring the workstation serial port

To configure the workstation serial port:

1. Connect a null modem F/F DB9 cable from a COM port on the workstation to the RS-232 serial port on the switch.
2. Configure the workstation serial port according to your platform:
   For a Windows workstation:
   a. Open the HyperTerminal application. Click **Start**, then select **Programs > Accessories > Communications > HyperTerminal**.
   b. Enter a name for the switch connection and choose an icon in the Connection Description window. Click **OK**.
   c. Enter the following COM Port settings in the COM Properties window, and click **OK**.
      - Bits per second: 9,600
      - Data Bits: 8
      - Parity: None
      - Stop Bits: 1
      - Flow Control: None

For a Linux workstation:

a. Set up minicom to use the serial port. Create or modify the `/etc/minirc.dfl` file with the following content.

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

b. Verify that all users have permission to run minicom. Review the `/etc/minicom.users` file and confirm that the line `ALL` exists or that there are specific user entries.

Apply power to the switch

⚠ **WARNING!** This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by Underwriters Laboratories (UL) and Canadian Standards Association (CSA).
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by Verband der Elektrotechnik (VDE), SEMKO, and DEMKO.

To power up a 8/20q Fibre Channel Switch, attach the AC power cord to the receptacle on the back of the switch and to the power source.

The switch runs its self-tests and begins normal operation—this may take a few minutes:

1. The switch LEDs (Input Power, Heartbeat, System Fault) illuminate followed by all port Logged-in LEDs. The Logged-in LEDs that illuminate indicate the ports that are enabled.
2. After a couple seconds the System Fault LED is extinguished while the Input Power LED and Heartbeat LED remain illuminated.
3. After approximately one minute, the POST executes and the Heartbeat LED is extinguished.
4. After about another minute, the POST is complete, all LEDs are extinguished except the Input Power LED and the Heartbeat LED:
   - The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.
   - The Heartbeat LED indicates the results of the POST. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry. If the Heartbeat LED blinks steadily about once per second, the POST was successful, and you can continue with the installation process. Any other blink pattern indicates that an error has occurred. For more information, see "Heartbeat LED blink patterns" (page 48).

Connect the management station or workstation to the switch

You can manage the switch using the SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, or the CLI. SAN Connection Manager requires at least one FC connection and an Ethernet connection to the switch. QuickTools and Enterprise Fabric Management Suite require an Ethernet connection to the switch. The CLI can use an Ethernet connection or a serial connection.

- If this switch is part of the 8Gb SAN Connection Kit installation:
  - **a.** Connect at least one FC cable from the management station to the switch, or to another switch in the same fabric.
  - **b.** Use a 10/100 Base-T straight cable to connect the switch Ethernet port to the LAN that connects your management station that will run SAN Connection Manager (see Indirect Ethernet in Figure 13).
- If this switch is a standalone installation and you plan to use QuickTools, Enterprise Fabric Management Suite, or the CLI, connect the switch Ethernet port to the workstation, in one of the following ways:
  - Indirect Ethernet connection from the workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable (Figure 13).
  - Direct Ethernet connection from the workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable (Figure 13).
  - Serial port connection from the workstation to the switch RS-232 serial port connector. This requires a null modem F/F DB9 cable (Figure 13). This connection supports the CLI only.

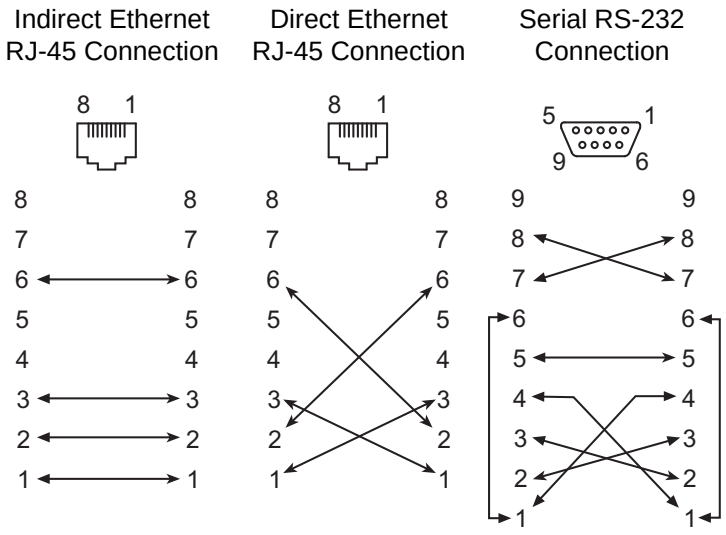


Figure 13 Management station and workstation cable connections

Configure the switch

You can configure the switch using SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, or the CLI.

SAN Connection Manager switch configuration

For information about installing the SAN Connection Manager application, see the *HP 8Gb SAN Connection Kit quick start instructions*. The SAN Connection Manager software will prompt you to set the switch IP address, administrator password, and default zoning when you first start that application.

When the configuration is complete, proceed to "Cable devices to the switch" (page 39).

QuickTools switch configuration

To log in and configure the switch using QuickTools:

1. Open an Internet browser and enter the default IP address 10.0.0.1 to start the QuickTools web applet.
2. Log in to the switch using the default user name (*admin*) and password (*password*).
3. Obtain the IP address and subnet mask from your network administrator.
4. Open the QuickTools Wizards menu and select **Configuration Wizard.** Follow the instructions to set the IP address and the password. Changing the IP address terminates the QuickTools session.
5. Open an Internet browser again and log in with the new IP address.
6. When the configuration is complete, proceed to "Cable devices to the switch" (page 39).

Enterprise Fabric Management Suite configuration

For information about downloading Enterprise Fabric Management Suite with a 30-day trial license, see the HP website www.hp.com/go/EFMS. For information about using Enterprise Fabric Management Suite application, see the *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*.

When the configuration is complete, proceed to "Cable devices to the switch" (page 39).

CLI switch configuration

To configure the switch using the command line interface.

1. Open a command window according to the type of workstation and connection.

   For an Ethernet connection (all platforms), open a Telnet session with the default switch IP address and log in to the switch with default account name and password (admin/password).

   ```
   telnet 10.0.0.1
   Switch Login: admin
   Password:     *******
   ```

   NOTE: To ensure user account security, change the password for the Admin account name. See the `passwd` command in the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*

   For a Windows serial connection, open the HyperTerminal application on a Windows platform.

   a. Click **Start**, then select **Programs > Accessories > Communications > HyperTerminal**.
   b. Select the connection you created earlier and click **OK**. See "Configuring the workstation serial port" (page 35).

   For a Linux serial connection, open a command window and enter the following command:

   ```
   minicom
   ```

2. Open an admin session and enter the `set setup system` CLI command. Enter the values you want for the switch IP address (EthNetworkAddress) and the network mask (EthNetworkMask). For more information about CLI commands, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

   ```
   8/20q FC Switch #> admin start
   8/20q FC Switch (admin) #> set setup system
   ```

3. Open a Config Edit session and use the `set config switch` CLI command to modify the switch configuration.
4. When the configuration is complete, proceed to "Cable devices to the switch" (page 39).

Cable devices to the switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers. Duplex cable connectors are keyed to ensure proper orientation. Choose the Fibre Channel cables with the connector combination that matches the device host bus adapter.

GL_Ports self configure as FL_Ports when connected to loop of devices or F_Ports when connected to a single device. G_Ports self-configure as F_Ports when connected to a single device. Both GL_Ports and G_Ports self-configure as E_Ports when connected to another switch.

Installing firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management station or workstation as new firmware becomes available using SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite, or the CLI. This guide describes the use of QuickTools and the CLI. For information about installing firmware using SAN Connection Manager, see the *HP SAN Connection Manager User Guide*. For information about installing firmware using Enterprise Fabric Management Suite, see the *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*.

You can load and activate firmware upgrades on an operating switch without disrupting data traffic or re-initializing attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the activation will fail. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

- The current firmware version supports the installation and non-disruptive activation of the new firmware. For information about compatible firmware versions, see the firmware release notes.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, changing switch configurations, or installing firmware.
- No port in the fabric is in the diagnostic state.
- No Zoning Edit sessions are open in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

If you are installing firmware on more than one switch in the fabric, wait until the activation is complete on the first switch before installing firmware on a second switch. If you attempt to activate firmware on a second switch before activation is complete on the first, you will receive a message advising you to wait and perform a hot reset later on the second switch to complete the installation.

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, SAN Connection Manager, QuickTools, Enterprise Fabric Management Suite sessions reconnect automatically. However, Telnet sessions must be restarted manually.

TIP: After upgrading firmware that includes changes to QuickTools, an open QuickTools session may indicate that the firmware is not supported. This means the new firmware is not supported by the previous QuickTools version. To correct this, close the QuickTools session and the browser window, then open a new QuickTools session.

Using QuickTools to install firmware

To install firmware using QuickTools:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Load Firmware dialog, choose one of the following:
   - Select a firmware image file from the Version drop-down list.
   - Click **Browse** to change the folder (path) to search for firmware image files. Click **Rescan** to search the new folder displayed in the Firmware Image Folder field.
3. Click **Start** to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
4. Click **OK** to continue firmware installation.
5. Click **Close** to close the Load Firmware dialog.

Using the CLI to install firmware

The method you choose to install firmware using the CLI depends on the type of firmware activation you want.

- For a disruptive activation, enter the `firmware install` or `image install` command to download the firmware image file from an FTP or TFTP server, unpack it, and activate it in one step. See "One-step firmware installation" (page 40).
- For a non-disruptive activation, enter the `image fetch` command to download the firmware image file from an FTP or TFTP server. Enter the `image unpack` command to unpack the image file, then enter the `hotreset` command to perform a non-disruptive activation. See "Custom firmware installation" (page 41).

For information about the CLI commands, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

One-step firmware installation

The `firmware install` and `image install` commands download the firmware image file from an FTP or TFTP server to the switch, unpack the image file, and perform a disruptive activation in one step. The installation process prompts you to enter the following:

- The file transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

For information about the CLI commands, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

1. Enter the following commands to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

```
8/20q FC Switch #> admin start
8/20q FC Switch #> firmware install
 The switch will be reset. This process will cause a
  disruption to I/O traffic.
 Continuing with this action will terminate all management
  sessions, including any Telnet sessions. When the firmware
  activation is complete, you may log in to the switch again.
 Do you want to continue? [y/n]: y
 Press 'q' and the ENTER key to abort this command.
```

2. Enter your choice for the file transfer protocol with which to download the firmware image file. FTP requires an user account and a password; TFTP does not.

```
FTP or TFTP      : ftp
```

3. Enter your account name on the remote host (FTP only) and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
User Account     : johndoe
IP Address       : 10.20.20.200
Source Filename : 8.0.4.xx.xx_epc
About to install image.  Do you want to continue? [y/n] y
```

4. When prompted to install the new firmware, enter `y` to continue or `n` to cancel. Entering `y` will disrupt traffic. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
```

5. Enter the password for your account name (FTP only).

```
331 Password required for johndoe.
Password:******
230 User johndoe logged in.
```

The firmware will now be downloaded from the remote host to the switch, installed, and activated.

Custom firmware installation

A custom firmware installation downloads the firmware image file from an FTP or TFTP server to the switch, unpacks the image file, and resets the switch in separate steps. This allows you to choose the type of switch reset and whether the activation will be disruptive (`reset switch` command) or nondisruptive (`hotreset` command). The following example illustrates a custom firmware installation with a nondisruptive activation.

1. Download the firmware image file from the server to the switch.
   - If your server has an FTP server, you can enter the `image fetch` command:

     ```
     8/20q FC Switch (admin) #> image fetch account_name ip_address
     filename
     ```

   - If your server has a TFTP server, you can enter the `image tftp` command to download the firmware image file.

     ```
     8/20q FC Switch (admin) #> image tftp ip_address filename
     ```

   - If your server has neither an FTP nor a TFTP server, open an FTP session and enter FTP commands:

     ```
     >ftp ip_address or switchname
     user:images
     password: images
     ftp>bin
     ftp>put filename
     ftp>quit
     ```

2. Display the list of firmware image files on the switch to confirm that the file was loaded.

   ```
   8/20q FC Switch (admin) $>image list
   ```

3. Unpack the firmware image file to install the new firmware in flash memory.

   ```
   8/20q FC Switch (admin) $>image unpack filename
   ```

4. Wait for the unpack to complete.

   ```
   image unpack command result: Passed
   ```

5. A message will prompt you to reset the switch to activate the firmware. Use the `hotreset` command to attempt a non-disruptive activation.

   ```
   8/20q FC Switch (admin) $>hotreset
   ```

Adding a switch to an existing fabric

If there are no special conditions to be configured for the new switch, plug in the switch. The switch becomes functional with the default fabric configuration. The default fabric configuration settings are as follows:

- Fabric zoning is sent to the switch from the fabric.
- All ports will be GL_Ports.
- The default IP address 10.0.0.1 is assigned to the switch without a gateway or boot protocol configured: Reverse Address Resolution Protocol (RARP) Bootstrap Protocol (BOOTP), and Dynamic Host Configuration Protocol (DHCP).

If you are adding a switch to a fabric and do not want to accept the default fabric configuration:

1. If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address.
3. Plug in the inter-switch links (ISL), but do not connect the devices.
4. Configure the port types for the new switch. The ports can be G_Port, GL_Port, F_Port, FL_Port, TR_Port, or Donor.
5. Connect the devices to the switch.
6. Make any necessary zoning changes.

Installing feature license keys

For information about available license keys, see "Feature licenses" (page 20). To install a license key using QuickTools:

1. Open the Switch Menu and select **Features** to open the Feature Licenses dialog.
2. In the Feature Licenses dialog, click **Add** to open the Add License Key dialog.
3. In the Add License Key dialog, enter the license key in the Key field.
4. Click **Get Description** to display the upgrade description.
5. Click **Add** to upgrade the switch. Allow a minute or two for the upgrade to complete.

To upgrade a switch using the command line interface, see the `feature` command in the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

Configuring Call Home to HP Services (optional)

Call Home to HP Services is supported for the 8/20q Fibre Channel Switch.

- If you have already configured Call Home to HP Services for other HP products using Remote Support Client (RSC), which is part of the Remote Support Pack (RSP), then to configure Call Home to HP Services for the 8/20q Fibre Channel Switch, you must add the switch as a managed system to HP Open Service Event Manager (OSEM) and then configure SNMP traps in the switch.
- If you have not already configured Call Home to HP Services, then you must set up a Central Management Server (CMS) to run HP Systems Insight Manager (SIM), which will direct the installation of RSP applications to support Call Home to HP Services.

Role of the Remote Support Software Manager

When you install RSP, Remote Support Software Manager (RSSWM) is also installed on your CMS. RSSWM downloads required and recommended software components, including the required software components listed below, which are used to allow communication with HP Services, contract and warranty entitlement capabilities and to provide on-site analysis.

- Remote Support Client (RSC)
- Remote Support Common Components (MC3)
- Remote Support Eligible Systems List
- Open Service Event Manager (OSEM)
- Web-Based Enterprise Services (WEBES)

These and other software management options you select are downloaded by RSSWM. Once configured, RSSWM will download and install updated versions as they become available according to the policies selected during the configuration of RSSWM.

Role of OSEM and versions required

OSEM collects and formats problem reports from various HP customer systems, including the 8/20q Fibre Channel Switch. OSEM uses the Ethernet (LAN) connection on the switches to receive event notifications through SNMP traps sent from the switches, and then sends automated notification messages to local e-mail recipients (if so configured) and to HP Services through RSC. These applications, in turn, send the event message over the internet to HP Services.

OSEM version1.4.5 and SIM 5.1 (which includes RSP version 5.05) are the minimum versions required to support 8/20q Fibre Channel Switch Call Home to HP Services.

Installation instructions and documentation for SIM, RSP, and OSEM

Software, installation instructions, release notes, and other documentation for SIM, RSP, and OSEM Standard Configuration are available at no charge from the following HP websites:

- For SIM at http: //www.hp.com/go/hpsim
- For RSP at http://www.hp.com/go/ServiceEssentials
- For OSEM at http://h18023.www1.hp.com/support/svctools/OSEM/index.html

RSP requirements for the CMS

RSP requires that the CMS be a Windows-based system with the following characteristics:

Hardware:

- Any HP ProLiant x86 or HP ProLiant x64 system
- 2.4-GHz processor minimum
- 3 GB RAM minimum; 4 GB RAM if more than 100 devices to be monitored
- 500 MB free disk space minimum

Operating system:

- Microsoft Windows 2000 Server, SP4 for x86
- Microsoft Windows 2000 Advanced Server, SP4 for X86
- Microsoft Windows Server 2003 Standard or Enterprise Edition for x86 with SP1 (running on x86 or x64/AMD64 platforms)
- Microsoft Windows Server 2003 for x64
- Microsoft Windows 2003 SMB, with SP1
- Microsoft Windows 2003 Server with installed Multilingual User Interface Pack (MUI)
- Microsoft Windows 2003 Server with English, French, Italian, German, Spanish and Dutch International Server

Supported Web browsers:

- Internet Explorer, Version 6.0 and 7.0
- Mozilla, Versions 1.5, 1.6, and 1.7
- Firefox, Versions 1.0.2, 1.5, and 2.0

Applications:

- Java Virtual Machine plug-in for Internet Explorer

NOTE: Java plug-in is not installed by default in the Internet Explorer Web Browser for 32-bit and x64 editions of Windows Server 2003.

Infrastructure requirements for implementing Call Home to HP Services

To implement Call Home to HP Services, the following infrastructure requirements must be met:

- Internet access to the Central Management Server running RSC. (Required because notification messages are sent by RSC to HP over the Internet.)
- OSEM can run on the same server as RSC or on a server that has LAN access to the server running RSC.
- The server running OSEM must have LAN access to the 8/20q Fibre Channel Switches to receive SNMP traps from the switches.
- If a fire wall is installed, the following ports must be open:
  - Port 162, which receives SNMP traps from the switches, because OSEM uses Microsoft SNMP services
  - Port 2069, to communicate with web browsers seeking remote access to OSEM

Configuring Call Home to HP services

To configure Call Home to HP services:

1. Make sure SIM and RSC are installed on a server that has Internet access. For software, installation instructions, and other documentation for SIM and RSP, see the HP websites listed in "Installation instructions and documentation for SIM, RSP, and OSEM" (page 43).
2. Make sure OSEM is installed on a server that has Ethernet access to the server running SIM and RSC, and to the 8/20q Fibre Channel Switches.

   NOTE: OSEM can also be installed on the server that is used to run SIM and RSC.

3. To enable a switch to Call Home to HP Services, configure an SNMP trap in the switch using QuickTools or the CLI, as described in the following procedures:

   To configure an SNMP trap using QuickTools:

   a. Enter the IP address of the switch into the web browser of a server that has LAN access to the switch, and login to the switch.
   b. To open the SNMP Properties dialog box: In the fabric tree, click the switch graphic for the switch you are configuring to open its faceplate display, and then select **Switch > SNMP Properties**.
   c. In the SNMP Properties dialog, select the tab for a trap that is not currently in use.
   d. In the display for the selected trap, select the **Trap Enabled** checkbox to enable the trap.
   e. In the Trap Version field, select the trap version **V1**.
   f. In the Trap Severity field, select **Critical**.
   g. In the Trap Address field, enter the IP address of the server running OSEM.
   h. In the Trap Port field, enter the trap port number used by OSEM (the OSEM default trap port is 162).

i. In the Trap Community field, enter the trap community name. The name can be up to 32 characters and must agree with the community name used in the OSEM application. The following characters may not be used in the user-defined fields: pound sign (#), semi-colon (;), and comma (,).

j. Click **OK** to enable the changes.

For more information about QuickTools, see the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*.

To configure an SNMP trap using the CLI:

a. Telnet to the IP address of the switch from a server that has LAN access to the switch, and login to the switch.

b. To modify the SNMP configuration, open an admin session and enter the `set setup snmp trap` CLI command. This will display the current configuration of SNMP trap parameters, followed by queries to allow changes to these parameters. Enter changes as needed to the trap enabled state, IP address, port number, severity, version, and community name.

The following example configures SNMP trap 1:

```
8/20q FC Switch #> admin start
8/20q FC Switch (admin) #> set setup snmp trap 1
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Current Values:
  Trap1Enabled    False
  Trap1Address    10.0.0.254
  Trap1Port       162
  Trap1Severity   warning
  Trap1Version    2
  Trap1Community  public

New Value (press ENTER to not specify value, 'q' to quit):
  Trap1Enabled    (True / False)                    :True
  Trap1Address    (hostname, IPv4, or IPv6 Address) :10.20.30.40
  Trap1Port       (decimal value, 1-65535)          :
  Trap1Severity   (select a severity level)
                  1=unknown      6=warning
                  2=emergency    7=notify
                  3=alert        8=info
                  4=critical     9=debug
                  5=error        10=mark            :4
  Trap1Version    (1 / 2)                           :1
  Trap1Community (string, max=32 chars)             :OSEMcommunity

Do you want to save and activate this snmp setup? (y/n): [n]
```

For more information about CLI commands, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

4. Configure the switches in OSEM by adding each 8/20q Fibre Channel Switch as a Managed System configured with System Type set to **FC Switch** and the IP address for the switch. For detailed instructions, see the OSEM documentation available at the web sites listed in "Installation instructions and documentation for SIM, RSP, and OSEM" (page 43).

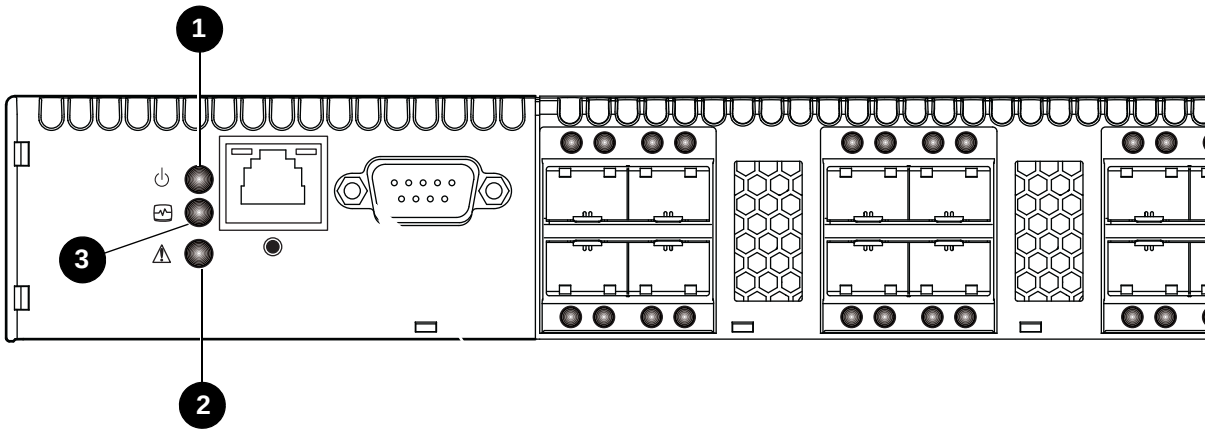
4 Diagnostics and Troubleshooting

Diagnostic information about the switch is available through the switch LEDs and the port LEDs. Diagnostic information is also available through the CLI, QuickTools, Enterprise Fabric Management Suite, or SAN Connection Manager event logs and error displays.

This chapter also describes using maintenance mode to recover a disabled switch. See "Recovering a switch using maintenance mode" (page 53).

Switch diagnostics

The 8/20q Fibre Channel Switch has three switch LEDs that are used for diagnostics: Input Power LED, Heartbeat LED, and the System Fault LED (Figure 14).



1 Input Power LED
2 System Fault LED
3 Heartbeat LED

Figure 14 Switch LEDs

Input power LED is extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished:

1. Inspect the power cords and connectors. Is the cord unplugged? Is the cord or connector damaged?
   - Yes—Make necessary corrections or repairs. If the condition remains, continue.
   - No—Continue.
2. Inspect the AC power source. Is the power source delivering the proper voltage?
   - Yes—Continue.
   - No—Make necessary repairs. If the condition remains, contact your authorized maintenance provider.

System fault LED is illuminated

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. If the System Fault LED illuminates, identify the Heartbeat LED error blink pattern and take the necessary actions. See "Heartbeat LED blink patterns" (page 48).

Power-On self test diagnostics

The switch performs a series of tests as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in Programmable read-only memory (PROM) and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the Application-specific integrated circuit (ASIC)

During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not. The switch uses the Heartbeat LED and the Logged-in LED to indicate switch and port status. A critical error disables the switch so that it will not operate. A non-critical error allows the switch to operate, but disables the ports that have errors. If two or more ports fail the POST, the entire switch is disabled. Whether the problem is critical or not, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a critical error occurs, the Heartbeat LED will show a blink pattern that indicates an error, and the System Fault LED will illuminate. If there are non-critical errors, the switch disables the failed ports and flashes the associated Logged-in LEDs. For more information, see "Heartbeat LED blink patterns" (page 48).

Heartbeat LED blink patterns

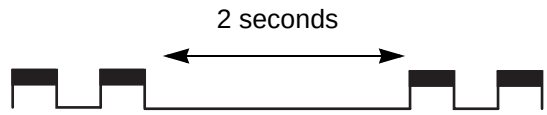
The Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. For more information, see "Recovering a switch using maintenance mode" (page 53). All other blink patterns indicate critical errors. In addition to producing a Heartbeat error blink patterns, a critical error also illuminates the System Fault LED.

The Heartbeat LED shows an error blink pattern for the following conditions:

- 1 blink—Normal operation
- 2 blinks—Internal firmware failure blink pattern, page 48
- 3 blinks—Fatal POST error blink pattern, page 48
- 4 blinks—Configuration file system error blink pattern, page 49
- 5 blinks—Over-temperature blink pattern, page 49

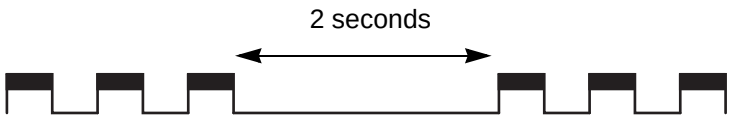
Internal firmware failure blink pattern

An internal firmware failure blink pattern is 2 blinks followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Momentarily press and release the Maintenance button to reset the switch.



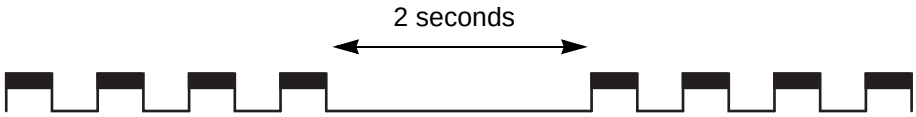
Fatal POST error blink pattern

A system error blink pattern is 3 blinks followed by a 2-second pause. The 3-blink error pattern indicates that a POST failure or a system error has left the switch inoperable. If a system error occurs, contact your authorized maintenance provider. Momentarily press and release the Maintenance button to reset the switch.



Configuration file system error blink pattern

A configuration file system error blink pattern is 4 blinks followed by a 2-second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be restored.



To restore the switch configuration:

1. Establish communications with the switch using Telnet. Enter one of the following on the command line:

   `telnet` *`xxx.xxx.xxx.xxx`*

   or

   `telnet` *`switchname`*

   where *`xxx.xxx.xxx.xxx`* is the switch IP address and *switchname* is the switch name associated with the IP address.
2. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are `admin` and `password` respectively.
3. Open an admin session to acquire the necessary authority.

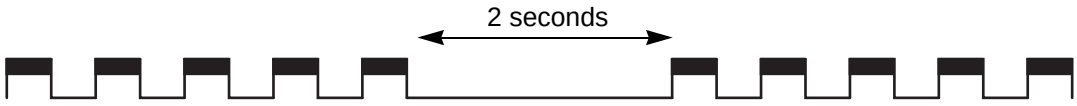
   ```
   8/20q FC Switch $> admin start
   ```
4. Restore the configuration. When the restore is complete, the switch will reset.

   ```
   8/20q FC Switch (admin) $> config restore
   ```

   If a configuration does not exist, enter the `config backup` CLI command, then enter the `config restore` command.

Over-temperature blink pattern

An over-temperature blink pattern is 5 blinks followed by a 2-second pause. The 5-blink error pattern indicates that the air temperature inside the switch has exceeded the failure temperature threshold.

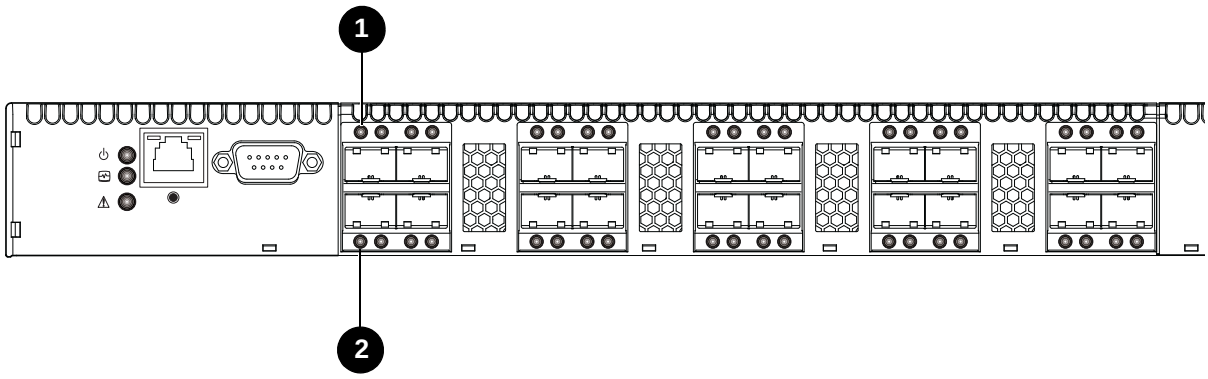


If the Heartbeat LED shows the over-temperature blink pattern:

1. Inspect the switch vents. Are the intake and exhaust vents clear?
   - Yes—Continue.
   - No—Remove any debris from fan intake and exhaust if necessary. If the condition remains, continue.
2. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, power down the switch and contact your authorized maintenance provider.

Logged-in LED indications

Port diagnostics are indicated by the Logged-in LED for each port (Figure 15).



1 Logged-in LED (port 0)

2 Logged-in LED (port 10)

Figure 15 Logged-in LED

The Logged-in LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: A device is logging in to the port, or the port is in the diagnostics state.
- Flashing twice per second: The port is down, offline, or an error has occurred.

If a Logged-in LED is flashing two times per second, review the event browser for alarm messages regarding the affected port. You can also inspect the alarm log using the command line interface, `show alarm` command. If there is an error, alarm messages may point to one or more of the following conditions:

- E_Port isolation, page 50
- Excessive port errors, page 51

E_Port isolation

A Logged-in LED error indication is often the result of E_Port isolation. E_Port isolation can be caused by the following:

- Security failure
- A port configured as an F_Port or an FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zonesets
- Connection to a B-series or C-series switch

Using QuickTools, review the event browser, and perform the following procedure to diagnose and correct an isolated E_Port:

1. Does the QuickTools event browser show an alarm about an invalid attach on the affected port?
   - Yes—If you have configured device security, review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
   - No—Continue.
2. Does the QuickTools event browser show a repeating alarm about an unsupported E_Port command on the affected port?
   - Yes—The port is configured as an FL_Port and connected to another switch. Correct the port connection or the port type.
   - No—Continue.

3. Display the fabric domain IDs using the `show domains` CLI command or by selecting the QuickTools **Switch** tab, **Summary** icon. Are all domain IDs in the fabric unique?
   - Yes—Continue.
   - No—Correct the domain IDs on the offending switches using the `set config switch` CLI command or the QuickTools Switch Properties dialog. Reset the port. If the condition remains, continue.
4. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the `show config switch` CLI command or by selecting the QuickTools **Switch** tab, **Advanced** icon. Is each timeout value the same on every switch?
   - Yes—Continue.
   - No—Correct the timeout values on the offending switches using the `set config switch` CLI command or selecting **Switch>Advanced Switch Properties** in QuickTools. Reset the port. If the condition remains, continue.
5. Display the active zoneset on each switch using the `zoning active` CLI command or by selecting the QuickTools **Active Zoneset** tab. Compare the zone membership between the two active zonesets. Are they the same?
   - Yes—Contact your authorized maintenance provider.
   - No—Deactivate one of the active zonesets or edit the conflicting zones so that their membership is the same, then reset the port. If the condition remains, contact your authorized maintenance provider.

NOTE: E_Port isolation can be caused by merging two fabrics whose active zonesets have two zones with the same name, but different membership.

6. Is the port connected to a switch that supports connection to a TR_Port of an 8/20q Fibre Channel Switch?
   - Yes—Configure the port as a TR_Port and map the local and remote fabric devices.
   - No—Contact your authorized maintenance provider.

Excessive port errors

The switch can monitor a set of port errors and generate alarms based on user-defined sample windows and thresholds. These port errors include the following:

- Cyclic Redundancy Check (CRC) errors
- Decode errors
- ISL connection count
- Device login errors
- Device logout errors
- Loss-of-signal errors

Port threshold alarm monitoring is disabled by default. For information about managing port threshold alarms, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

If the count for any of these errors exceeds the rising trigger for three consecutive sample windows, the switch generates an alarm and disables the affected port, changing its operational state to “down.” Port errors can be caused by the following:

- Triggers are too low or the sample window is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Faulty device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then perform the following procedure:

1. Examine the alarm configuration for the associated error using the `show config threshold` CLI command. See the `show config threshold` CLI command in the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*. Are the thresholds and sample window correct?
   - Yes—Continue
   - No—Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. For information about testing ports, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide* or the *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*. Does the port pass the test?
   - Yes—Continue
   - No—Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.
3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes—The procedure is complete.
   - No—Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

Transceiver diagnostics

You can display the following transceiver information using the `show media` CLI command:

- Port number
- Manufacturer
- Temperature (°C)
- Operating voltage (volts)
- Transmitter bias (milliamps)
- Transmitter power (milliwatts)
- Receiver power (milliwatts)

The display indicates warning and alarm conditions for both high and low values.

Recovering a switch using maintenance mode

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Password is forgotten

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Exiting the maintenance menu (option 0), page 53
- Unpacking a firmware image file in maintenance mode (option 1), page 54
- Resetting the network configuration in maintenance mode (option 2), page 54
- Resetting user accounts in maintenance mode (option 3), page 54
- Copying log files in maintenance mode (option 4), page 54
- Removing the switch configuration in maintenance mode (option 5), page 54
- Remaking the file system in maintenance mode (option 6), page 54
- Resetting the switch in maintenance mode (option 7), page 55
- Updating the boot loader in maintenance mode (option 8), page 55

To recover a switch:

1. Place the switch in maintenance mode by pressing and holding the Maintenance button with a pointed tool until only the Heartbeat LED is illuminated, and then release the button. The Heartbeat LED illuminates continuously when the switch is in maintenance mode.
2. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
3. Enter the maintenance mode account name (`prom`) and password (`prom`), and press **Enter**.

```
Switch login: prom
Password:xxxx
```

4. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press **Enter**.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option:
```

These options and their use are described in the following subsections.

Exiting the maintenance menu (option 0)

The **Exit** option closes the current Maintenance menu session. To log in again, enter the maintenance mode account name (`prom`) and password (`prom`). To return to normal operation, momentarily press and release the Maintenance button or power cycle the switch.

Unpacking a firmware image file in maintenance mode (option 1)

The **Image Unpack** option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. To install new firmware using this option:

1. Place the switch in maintenance mode. See the procedure for maintenance mode in "Recovering a switch using maintenance mode" (page 53).
2. Use FTP to load a new firmware image file onto the switch. See "Custom firmware installation" (page 41) for an example of how to load the image file. When the download is complete, close the FTP session.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

   ```
   telnet 10.0.0.1
   ```

4. Enter the maintenance mode account name (`prom`) and password (`prom`), and press **Enter**.

   ```
   Switch login: prom
   Password: xxxx
   ```

5. Select option 1 from the maintenance menu. When prompted for a file name, enter the firmware image file name:

   ```
   Image filename: filename
   Unpacking 'filename', please wait...
   Unpackage successful.
   ```

6. Select option **7, Reset Switch**, to reset the switch and exit maintenance mode.

Resetting the network configuration in maintenance mode (option 2)

The **Reset Network Config** option resets the network properties to the factory default values and saves them on the switch. For default network configuration values, see "Factory Configuration Defaults" (page 71).

Resetting user accounts in maintenance mode (option 3)

The **Reset User Accounts to Default** option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

Copying log files in maintenance mode (option 4)

The **Copy Log Files** option copies all log file buffers to a file on the switch named `logfile`. You can use FTP to download this file to the workstation, however, you must download `logfile` before resetting the switch. For information about downloading files from the switch, see the *HP 8/20q Fibre Channel Switch Command Line Interface Guide*.

Removing the switch configuration in maintenance mode (option 5)

The **Remove Switch Config** option deletes all configurations from the switch except the default configuration. This restores switch configuration parameters to the factory defaults. See "Factory Configuration Defaults" (page 71) for the factory default values.

Remaking the file system in maintenance mode (option 6)

The **Remake Filesystem** option resets the switch to the factory default values, including user accounts and zoning. Use this option to recreate the file system when the switch configuration becomes corrupt because of a loss of power. See "Factory Configuration Defaults" (page 71) for the factory default values.

NOTE: If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

Resetting the switch in maintenance mode (option 7)

The **Reset Switch** option closes the Telnet session, exits maintenance mode, and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Updating the boot loader in maintenance mode (option 8)

The **Update Boot Loader** option updates the system boot loader which loads the Linux kernel into memory. Use this option only at the direction of your authorized maintenance provider.

5 Support and Other Resources

Document conventions and symbols

Table 10 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and email addresses
Medium blue, underlined text (http://www.hp.com)	Website addresses
Bold font	• Keys that are pressed • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of monospace text, including file and directory names, system output, code, and text typed at the command line

WARNING! Indicates that failure to follow directions could result in bodily harm or death.

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Contacting HP

HP contact information

For HP technical support:

- In the United States, see the Contact HP United States webpage: (http://welcome.hp.com/country/us/en/contact_us.html). To contact HP by phone, call: 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
- In other locations, see the Contact HP worldwide (in English) webpage: (http://www.hp.com/country/us/en/wwcontact.html).
- For worldwide technical support information, see the HP support website: http://www.hp.com/support/.

Rack stability

⚠ **WARNING!** To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, secure racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website: http://www.hp.com/go/e-updates. After registering, you will receive an e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, send a message to storagedocs.feedback@hp.com. Include the document title and manufacturing part number. All submissions become the property of HP.

New and changed information in this edition

The following additions and changes have been made for this edition:

- Added support for the Enterprise Fabric Management Suite fabric management application
- Added support for the port activation license key

Related information

Documents

In addition to this guide, see the following documents for this product:

- *HP 8/20q and SN6000 Fibre Channel Switch Quick Start Installation Instructions*
- *HP 8/20q and SN6000 Fibre Channel Switch Rack Mount Kit Quick Start Installation Instructions*
- *HP 8/20q and SN6000 Fibre Channel Switch Rack-Mount Kit quick start installation instructions*
- *HP 8Gb SAN Connection Kit Quick Start Instructions*
- *HP 8/20q Fibre Channel Switch QuickTools Switch Management User Guide*
- *HP 8/20q Fibre Channel Switch Command Line Interface Guide*

- *HP 8/20q and SN6000 Fibre Channel Switch Command Line Interface Quick Reference Guide*
- *HP 8/20q and SN6000 Enterprise Fabric Management Suite User Guide*
- *HP SAN Connection Manager User Guide*
- *HP 8/20q an SN6000 Fibre Channel Switch Event Messages Reference Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch Simple Network Management Protocol Reference Guide*
- *HP 8/20q and SN6000 Fibre Channel Switch CIM Agent Reference Guide*

For the latest product information, including firmware, documentation, and supported SAN configurations, see the following HP website: http://www.hp.com/go/8Gb-SSC.

Other HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.docs.hp.com
- http://www.hp.com/go/sandesignguide

Customer self repair

HP products are designed with many Customer Self Repair parts to minimize repair time and allow for greater flexibility in performing defective parts replacement. If during the diagnosis period HP (or HP service providers or service partners) identifies that the repair can be accomplished by the use of a Customer Self Repair part, HP will ship that part directly to you for replacement. There are two categories of Customer Self Repair parts:

- Mandatory—Parts for which Customer Self Repair is mandatory. If you request HP to replace these parts, you will be charged for the travel and labor costs of this service.
- Optional—Parts for which Customer Self Repair is optional. These parts are also designed for customer self repair. If, however, you require that HP replace them for you, there may or may not be additional charges, depending on the type of warranty service designated for your product.

NOTE:

Some HP parts are not designed for Customer Self Repair. In order to satisfy the customer warranty, HP requires that an authorized service provider replace the part. These parts are identified as No in the Illustrated Parts Catalog.

Based on availability and where geography permits, Customer Self Repair parts will be shipped for next business day delivery. Same day or four-hour delivery may be offered at an additional charge where geography permits. If assistance is required, you can call the HP Technical Support Center and a technician will help you over the telephone. HP specifies in the materials shipped with a replacement Customer Self Repair part whether a defective part must be returned to HP. In cases where it is required to return the defective part to HP, you must ship the defective part back to HP within a defined period of time, normally five (5) business days. The defective part must be returned with the associated documentation in the provided shipping material. Failure to return the defective part may result in HP billing you for the replacement. With a Customer Self Repair, HP will pay all shipping and part return costs and determine the courier/carrier to be used.

For more information about the HP Customer Self Repair program, contact your local service provider. For the North American program, visit the HP website (http://www.hp.com/go/selfrepair).

A Regulatory Compliance and Safety

Regulatory compliance

Federal Communications Commission notice for Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Laser device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light.

⚠ **WARNING!**

To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the laser device.

Laser safety warning

This product uses Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

Certification and classification information

This product contains a laser internal to the fiber optic (FO) transceiver for connection to the Fibre Channel communications port.

In the USA, the FO transceiver is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. A label on the plastic FO transceiver housing indicates the certification.

Outside the USA, the FO transceiver is certified as a Class 1 laser product conforming to the requirements contained in IEC 825–1:1993 and EN 60825–1:1994, including Amendment 11:1996 and Amendment 2:2001.

Laser product label

The optional Class 1 laser product label (Figure 16) or its equivalent may be located on the surface of the HP-supplied laser device or on the laser device installed in your product.

Figure 16 Class 1 laser product label

This label indicates that the product is classified as a CLASS 1 LASER PRODUCT.

International notices and statements

Canadian notice (avis Canadien)

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

European Union regulatory notice

This product complies with the following Eurupean Union (EU) directives:

- Low Voltage Directive 2006/95/EC
- EMC Directive 2004/108/EC

Compliance with these directives implies conformity to applicable harmonized European standards (European norms), which are listed on the *EU Declaration of Conformity* issued by Hewlett-Packard for this product or product family. This compliance is indicated by the following conformity marking placed on the product:

CE This marking is valid for non-telecommunications products and EU harmonized telecommunications products.	CE XXXX* ! This marking is valid for EU non-harmonized telecomunications products. *Notified body number (used only if applicable—refer to the product label)

Hewlett-Packard GmbH, HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, Germany

Japanese notice

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean notice

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Taiwan notice

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

Chinese warning messages

Altitude warning message

仅适用于海拔 2000 米以下地区安全使用

May be used safely only in areas where the altitude is less than 2000m.

Non-tropical warning message

仅适用于非热带气候条件下安全使用

May be used safely only in non-tropical climates.

B How to Prevent Electrostatic Discharge

To prevent damage to the system, you must follow certain precautions when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always make sure you are properly grounded when touching a static-sensitive component or assembly.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or static-dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an HP authorized reseller install the part.

NOTE: For more information on static electricity, or for assistance with product installation, contact your HP authorized reseller.

C Technical Specifications

This appendix contains the specifications for the 8/20q Fibre Channel Switch. See "General Description" (page 7) for the location of all connections, switches, controls, and components.

General specifications

Table 11 lists general specifications for the 8/20q Fibre Channel Switch.

Table 11 General specifications for the 8/20q Fibre Channel Switch

Specification	Description
Fibre Channel protocols	FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-FLA FC-GS FC-GS-2 FC-GS-3 FC-FG FC-SW-2 FC-Tape FC-VI Fibre Alliance MIB Version 4.0 Fibre Channel Element MIB RFC 2837\
Fibre Channel classes of service	Classes 2 and 3
Modes of operation	Fibre Channel Classes 2 and 3, connectionless
Port types	G_Port, GL_Port, F_Port, FL_Port, E_Port, TR_Port
Port characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel ports	Available as 8-port and 16-port base models with license key upgrades to 12, 16, and 20 ports.
Scalability	Maximum 239 switches, depending on configuration. For the latest supported configurations, see the *SAN Design Reference Guide* available at http://www.hp.com/go/SANdesignguide.

Table 11 General specifications for the 8/20q Fibre Channel Switch (Continued)

Specification	Description
Maximum user ports	> 475,000 ports depending on configuration. For the latest supported configurations, see the *SAN Design Reference Guide* available at http://www.hp.com/go/SANdesignguide.
Buffer credits	16 buffer credits per port, ASIC embedded memory
Media type	SFP optical transceiver
Fabric port speed	2.125, 4.250, 8.50 Gb/s
Maximum frame size	2148 bytes (2112 byte payload)
System processor	440EP PowerPc
Fabric latency (intra-switch) 2 Gb/s to 2 Gb/s 4 Gb/s to 4 Gb/s 8 Gb/s to 8 Gb/s	 < 0.6 µsec < 0.3 µsec < 0.2 µsec
Bandwidth Point-to-point Aggregate (single switch)	 425 MB, Full Duplex @ 2 Gb/s 850 MB, Full Duplex @ 4 Gb/s 1,700 MB, Full Duplex @ 8 Gb/s Up to 34 GB Full Duplex
Air flow	Front-to-back

Maintainability features

Table 12 Maintainability feature for the 8/20q Fibre Channel Switch

Specification	Description
Diagnostics	The POST tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User interface	LED indicators
Field replaceable units (FRUs)	None

Fabric management specifications

Table 13 Fabric management specifications for the 8/20q Fibre Channel Switch

Specification	Description
Management methods	Command Line Interface FTP GS-3 Management Server SAN Connection Manager graphical user interface QuickTools web applet SMI-S SNMP TFTP
Maintenance connection	RS-232 connector; null modem F/F DB9 cable
Ethernet connection	RJ-45 connector; 10/100 BASE-T cable
Switch agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

Weight and physical dimensions

Table 14 Switch physical dimensions for the 8/20q Fibre Channel Switch

Property	Value
Height	1U or 43.2 mm (1.70 in)
Width	432 mm (17 in)
Depth	305 mm (12.0 in)
Weight	4.08 kg (9 lb) with zero SFPs installed

Electrical specifications

Table 15 Electrical specifications for the 8/20q Fibre Channel Switch

Specification	Description
Operating voltage	100 to 240 VAC; 50 to 60 Hz
Power source loading (maximum)	1 A at 120 VAC/0.5 A at 240 VAC
Heat output (maximum)	100 watts
Circuit protection	Internally fused

Environmental requirements

To ensure proper operation, the switch must not be subjected to environmental conditions beyond those for which it was tested. The ranges specified in Table 16 identify the acceptable environment for both operating and non-operating conditions.

Table 16 Environmental requirements

Condition	Acceptable range during operation	Acceptable range during non-operation
Temperature	0° to 40°C (32° to 104°F)	-40° to 70°C (-40° to 158°F)
Humidity	15% to 80%, non-condensing	5% to 90%, non-condensing
Altitude	3,048 m (10,000 feet) above sea level	15,240 m (50,000 feet) above sea level
Vibration (IEC 68-2-6)	5-500 Hz, random, 0.21 Grms, 10 minutes	5-500 Hz, random, 2.1 Grms, 10 minutes
Shock (IEC 68-2-7)	4 g, 11ms, 20 repetitions	30 g, 292 ips, 13 msec, 3 square waves

D Factory Configuration Defaults

This appendix describes the factory configuration defaults:

Factory switch configuration

Enter the `show config switch` CLI command to display switch configuration values.

Table 17 Switch configuration defaults

Parameter	Default
AdminState	Online
BroadcastEnabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1,000
DefaultDomainID	1 (0x Hex)
DomainIDLock	False
SymbolicName	8/20q FC Switch
R_A_TOV	10000
E_D_TOV	2000
PrincipalPriority	254
ConfigDescription	Default Config
InteropMode	Standard

Factory port configuration

Enter the `show config port` CLI command to display port configuration values.

Table 18 Port configuration defaults

Parameter	Port Defaults
AdminState	Online
LinkSpeed	Auto
PortType	GL
SymbolicName	Port *n*, where *n* is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
AutoPerfTuning	True
LCFEnable	False
MFSEnable	False
MSEnable	True
NoClose	False
IOStreamGuard	Auto
VIEnable	False
PDISCPingEnable	True

Factory port threshold alarm configuration

Enter the `show config threshold` CLI command to display threshold alarm configuration values. If the ThresholdMonitoringEnabled parameter is disabled (False), none of the individual threshold monitoring parameter settings can be applied.

Table 19 Port threshold alarm configuration defaults

Parameter	Default
`ThresholdMonitoringEnabled`	`False`

`CRCErrorsMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`25`
	`1`
	`10`

`DecodeErrorsMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`25`
	`0`
	`10`

`ISLMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`2`
	`0`
	`10`

`LoginMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`5`
	`1`
	`10`

`LogoutMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`5`
	`1`
	`10`

`LOSMonitoringEnabled`
• `RisingTrigger`
• `FallingTrigger`
• `SampleWindow`
	`True`
	`100`
	`5`
	`10`

Factory zoning configuration

Enter the `show config zoning` CLI command to display zoning configuration values.

Table 20 Zoning configuration defaults

Parameter	Default
`MergeAutoSave`	`True`
`DefaultZone`	`Allow`
`DiscardInactive`	`False`

Factory SNMP configuration

Enter the `show setup snmp` CLI command to display SNMP configuration values.

Table 21 SNMP configuration defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	HP 8/20q Fibre Channel Switch
ObjectID	1.3.6.1.4.1.3873.1.11
AuthFailureTrap	False
ProxyEnabled	True
SNMPv3Enabled	False
Trap [1-5] Address	Trap 1: 10.0.0.254 Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False

Factory switch services configuration

Enter the `show setup services` CLI command to display switch service configuration values.

Table 22 Services configuration defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True
MgmtServerEnabled	True
CallHomeEnabled	True

Factory DNS host name configuration

Enter the `show setup system dns` CLI command to display the Domain Name System host name configuration values.

Table 23 DNS host name configuration defaults

Parameter	Default
DNSClientEnabled	False
DNSLocalHostname	<undefined>
DNSServerDiscovery	Static
DNSServer1Address	<undefined>
DNSServer2Address	<undefined>
DNSServer3Address	<undefined>
DNSSearchListDiscovery	Static
DNSSearchList1	<undefined>
DNSSearchList2	<undefined>
DNSSearchList3	<undefined>
DNSSearchList4	<undefined>
DNSSearchList5	<undefined>

Factory IP version 4 Ethernet configuration

Enter the `show setup system ipv4` CLI command to display the IP version 4 Ethernet configuration values.

Table 24 IP version 4 Ethernet configuration defaults

Parameter	Default
EthIPv4NetworkEnable	True
EthIPv4NetworkDiscovery	Static
EthIPv4NetworkIPAddress	10.0.0.1
EthIPv4NetworkIPMask	255.0.0.0
EthIPv4GatewayAddress	10.0.0.254

Factory IP version 6 Ethernet configuration

Enter the `show setup system ipv6` CLI command to display the IP version 6 Ethernet configuration values.

Table 25 IP version 6 Ethernet configuration defaults

Parameter	Default
EthIPv6NetworkEnable	True
EthIPv6NetworkDiscovery	Ndp
EthIPv6NetworkAddress	::/64
EthIPv6GatewayAddress	::

Factory event logging configuration

Enter the `show setup system logging` CLI command to display the event logging configuration values.

Table 26 Event logging configuration defaults

Parameter	Default
`LocalLogEnabled`	`True`
`RemotelogEnabled`	`False`
`RemoteLogHostAddress`	`10.0.0.254`

Factory NTP server configuration

Enter the `show setup system ntp` CLI command to display the NTP server configuration values.

Table 27 NTP server configuration defaults

Parameter	Default
`NTPClientEnabled`	`False`
`NTPServerAddress`	`10.0.0.254`
`NTPServerDiscovery`	`Static`

Factory timer configuration

Enter the `show setup system timers` CLI command to display the timer configuration values.

Table 28 Timer configuration defaults

Parameter	Default
`AdminTimeout`	`30`
`InactivityTimeout`	`0`

Factory RADIUS configuration

Enter the `show setup radius` CLI command to display RADIUS configuration values.

Table 29 RADIUS configuration defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	0
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Factory security configuration

Enter the `show config security` CLI command to display security configuration values.

Table 30 Security configuration defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	False
PortBindingEnabled	False

Factory Call Home configuration

Enter the `show setup callhome` CLI command to display call home configuration values.

Table 31 Call Home service configuration defaults

Parameters	Default
PrimarySMTPServerAddr	0.0.0.0
PrimarySMTPServerPort	25
PrimarySMTPServerEnabled	False
SecondarySMTPServerAddr	0.0.0.0
SecondarySMTPServerPort	25
SecondarySMTPServerEnabled	False
ContactEmailAddress	nobody@localhost.localdomain
PhoneNumber	<undefined>
StreetAddress	<undefined>
FromEmailAddress	nobody@localhost.localdomain
ReplyToEmailAddress	nobody@localhost.localdomain
ThrottleDupsEnabled	True

Glossary

This glossary defines terms used in this guide or related to this product. It is not a comprehensive glossary of computer terms.

4-port Upgrade License A licensed feature that enables you to activate additional FC ports.

Active firmware The firmware image on the switch that is in use.

Active zoneset The zoneset that defines the current zoning for the fabric. See Zoneset.

Activity LED A port LED that indicates when frames are entering or leaving the port.

Administrative state Assigned state that determines the operational state of the port or switch. There are two types of adminstrative states: the administrative state and the configured administrative state. The administrative state is the currently assigned port or switch state, such as `Online` or `Offline`. The configured administrative state is the state that is saved in the switch configuration, which determines how the switch or port comes up after a reset or power cycle.

Alarm A message generated by the switch that requires attention.

Alias A named set of ports or devices used to make defining zoneset membership easier. An alias is not a zone, and it cannot have a zone or another alias as a member. See Zone.

Application-specific integrated circuit (ASIC) An integrated ciruit chip designed for a specific application, such as a transmission protocol or a computer.

Arbitrated loop A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA) A unique one-byte value assigned during loop initialization to each NL_Port on a loop. See NL_Port.

BootP Boot strap protocol. A type of network server.

Buffer credit A measure of port buffer capacity, equal to one frame.

Challenge-Handshake Authentication Protocol (CHAP) An authentication protocol by which a device is challenged to verify its identity before being allowed to log in to a switch.

Class 2 service A service that multiplexes frames at frame boundaries to or from one or more N_Ports with acknowledgment provided. See N_Port.

Class 3 service A service that multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment. See N_Port.

Common Information Model (CIM) A switch service that provides for switch management through third-party applications that comply with the Storage Management Initiative–Specification (SMI-S).

Configuration wizard QuickTools or Enterprise Fabric Management Suite wizard that automates the switch configuration process.

Device security A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets. See Group and Security set.

Domain ID User-defined number that identifies the switch in the fabric.

Enterprise Fabric Management Suite An optional, workstation-based, fabric management application.

E_Port Expansion port. A Fibre Channel port that connects to another switch.

Event log Log of messages describing events that occur in the fabric.

Extended credits A feature of Enterprise Fabric Management Suite that enables the reallocation port buffer credits to extend transmission distances.

F_Port Fabric port. A Fibre Channel switch port that supports a connection to a single server or storage device.

Fabric device management interface (FDMI)	An interface by which device host bus adapters (HBAs) can be managed through the fabric.
Fabric management switch	The switch through which the fabric is managed.
Fabric security	A feature that provides security for fabric users and devices, including user account security and fabric services. See Device security and Fabric services.
Fabric services	A component of fabric security that provides for the control of inband management and SNMP on a switch. See Fabric security and Simple Network Management Protocol (SNMP).
FC port	Fibre Channel port
FL_Port	Fabric loop port. A Fibre Channel switch port that supports a connection to up to 126 server or storage devices.
Flash memory	Memory on the switch that contains the switch control firmware.
Frame	Data unit consisting of start-of-frame (SOF) delimiter, header, data payload, CRC, and end-of-frame (EOF) delimiter.
Group	A list of device worldwide names that are authorized to attach to a switch. There are three group types: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).
Heartbeat LED	A switch LED that indicates the status of the internal switch processor and the results of the Power-on self test.
Host bus adapter (HBA)	A circuit board that is installed in a server or storage device through which the device connects to the fabric.
IKE peer	The device connected to a switch that requires secure IP communication. The IKE configuration associated with this device that establishes an IKE security association connection with the switch. See Internet Key Exchange (IKE).
IKE policy	An IKE profile that defines the type of data traffic to secure between the switch and the peer, and how to encrypt that data. See Internet Key Exchange (IKE).
Inband management	The ability to manage a switch through another switch over an inter-switch link.
Initiator	The device that initiates a data exchange with a target device.
In-order-delivery	A feature that requires that frames be received in the same order in which they were sent.
Input power LED	A switch LED that indicates that the switch logic circuitry is receiving proper DC voltages.
Inter-Fabric Zone (IFZ)	A zone that is used to map local devices to devices on a remote HP B-series or C-series fabric across a TR_Port. The zone membership consists of the port WWNs of the local device, the remote device, and the TR_Port. The zone name is a concatenation of the IFZ prefix, the lowest WWN, and the remaining WWN, separated by underscores (_).
Internet Key Exchange (IKE)	A protocol that automates the sharing of encryption keys and algorithms through the configuration of matching IP security associations on the switch and on the connected device or peer. See IKE peer and IKE policy.
Inter-switch link (ISL)	The connection between two switches using E_Ports. See E_Port.
IP Security	Encryption-based security for IPv4 and IPv6 communications through security policies and security associations. See Security association and Security policy.
License key	A code associated with a separately-purchased feature that activates that feature on the switch.
Light Emitting Diode (LED)	One of several small lights that indicate the condition of the switch or a Fibre Channel port. See Heartbeat LED, Input power LED, System Fault LED, Activity LED, and Logged-in LED.
Logged-in LED	A Fibre Channel port LED that indicates the logged-in or initialization status of the connected devices.
Maintenance button	Momentary button on the switch used to reset the switch or place the switch in maintenance mode. See Maintenance mode.

Maintenance mode	Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.
Management Information Base (MIB)	A set of guidelines and definitions for SNMP functions. See Simple Network Management Protocol (SNMP).
Management station	Workstation or server used to run SAN Connection Manager.
N_Port	Node port. A Fibre Channel device port in a point-to-point or fabric connection.
Network Time Protocol (NTP)	A network protocol that enables a client to synchronize its time with a server.
NL_Port	Node loop port. A Fibre Channel device port that supports arbitrated loop protocol.
N-Port ID Virtualization (NPIV)	A Fibre Channel facility allowing multiple N_Port IDs to share a single physical N_Port.
Pending firmware	The firmware image that will be activated upon the next switch reset.
Port binding	An authorization method that defines a list of device WWNs that can login to a switch port. See Worldwide Name (WWN).
Power-on self test (POST)	Diagnostics that the switch performs at start up.
Principal switch	The switch in the fabric that manages domain ID assignments. See Domain ID.
QuickTools	A browser-based switch management application that resides in the switch firmware.
Remote Authentication Dial-in Service (RADIUS)	A service that supports the remote authentication of user and device logins to a switch.
Secure shell (SSH)	A protocol that secures connections to the switch for the command line interface.
Secure socket layer (SSL)	A protocol that secures connections to the switch for QuickTools, Enterprise Fabric Management Suite, and SMI-S.
Security association	An IP security profile that defines the encryption algorithm and encryption key to apply when called by a security policy. See IP Security.
Security policy	An IP security profile that defines host-to-host, host-to-gateway, and gateway-to-gateway connections; one policy for each direction. See IP Security.
Security set	A set of up to three groups containing no more than one of each group type: ISL, Port, or MS. The active security set defines the device security for a switch. See Group.
Simple Network Management Protocol (SNMP)	An application protocol that manages and monitors network communications and functions. It also controls the Management Information Base (MIB). See Management Information Base (MIB).
SAN Connection Manager (SCM)	A management application that provides basic automated configuration and management of switches, HBAs, and storage devices.
Small form-factor pluggable (SFP)	A transceiver device, smaller than a GigaBit interface converter, that plugs into the Fibre Channel port.
Storage Management Initiative–Specification (SMI-S)	A standard that provides for the management of the switch through third-party management applications.
System Fault LED	A switch LED that indicates that a fault exists in the switch firmware or hardware.
Target	A storage device that responds to an initiator device.
TR_Port	Transparent routing port. A port type that uses the Fibre Channel industry standard NPIV to provide access to devices on a remote HP B-series or C-series fabric.
User account	An object stored on a switch that consists of an account name, password, authority level, and expiration date.
User account security	A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.

Workstation	PC or Linux workstation that manages the switch using QuickTools or the command line interface (CLI).
Worldwide Name (WWN)	A unique 64-bit address assigned to a device by the device manufacturer.
Zone	A set of ports or devices grouped together to control the exchange of information.
Zoneset	A set of zones grouped together. The active zoneset defines the zoning for a fabric. See Zone.
Zoning database	The set of zonesets, zones, and aliases stored on a switch. See Alias, Zone, and Zoneset.

Index

Numerics

10/100 Base-T straight cable 37

A

account name
  default 38
  FTP 41
  maintenance mode 53
active zone set 17
Activity LED 11, 12
air flow 68
alias 17
altitude 70
association 25
authority 25
authorization 26

B

bandwidth 19, 68
boot loader 55
browser 29, 30
buffer credit 18, 68

C

cable
  10/100 Base-T 37
  10/100 Base-T crossover 37
  null modem F/F DB9 37
cable length 18
Call Home service
  configure to HP service 42
  description 24
certificate 25, 26
certificate authority 25
classes of service 67
command line interface 14
Common Information Model 23
configuration
  file system error 9, 49
  remove 54
  restore default 54
controls 8
conventions
  document 57
  text symbols 57
credits 18, 68
critical error 48

D

device
  access 17
  authentication 26
  authorization 26
  cabling 39
  description 17
  performance 20
  security 26
diagnostics 47, 48, 68
digital certificate 25
dimensions 69
disk space 29
distance 18
document conventions 57
documentation, HP website 59
domain ID
  conflict 51
  description 21
  lock 21

E

E_Port 11, 50
e-mail notification 24
encryption 25
Enterprise Fabric Management Suite 14
environmental
  conditions 30
  specifications 70
error
  critical 48
  fatal POST 48
  port 51
Ethernet
  direct connection 37
  indirect connection 37
  port 12

F

F_Port 11
fabric
  management 27, 69
  management switch 12
  point-to-point bandwidth 68
  port 11
  security 25
factory defaults 54
Fibre Channel
  ports 10
  protocols 67
Field Replaceable Unit 68
File Transfer Protocol
  account name 41
  description 15
  service 23
firmware
  description 39
  failure 48

install with CLI 40
install with QuickTools 40
non-disruptive activation 39
unpack image 54
FL_Port 11
flash memory 9
frame size 68
FRU - See Field Replaceable Unit
FTP - See File Transfer Protocol

G

G_Port 11
generic ports 11
GL_Port 11

H

hardware requirements 29, 30
HBA - See Host Bus Adapter
Heartbeat LED 8, 48
heat output 69
help, obtaining 58, 59
HP
services 42
storage website 59
Subscriber's choice website 58
technical support 58
humidity 30, 70
HyperTerminal application 35

I

IKE - See Internet Key Exchange
inband management 23
Input Power LED 47
installation 30
Inter-Fabric Zone 23
internal firmware failure 48
internet browser 29, 30
Internet Key Exchange 25
IP security 25

L

latency 19, 68
LED
Activity 11, 12
Heartbeat 8, 48
Input Power 8, 47
Link Status 12
Logged-In 10
Logged-in 50
System Fault 8, 47
license key 10, 42
Link Status LED 12
log file 54
Logged-in LED 10, 50
login limit 27

M

maintainability 68
maintenance
button 8, 9, 53
interface 69
menu 53
mode 9, 48, 53
Management Server 24
management station
connecting 37
requirements 29
media type 68
memory
flash 9
workstation 29
minicom 36
multiple switch fabrics 20

N

non-critical error 48
non-disruptive activation 39
N-Port ID Virtualization 21, 22
NTP - See Network Time Protocol
null modem F/F DB9 cable 37

O

Open Service Event Manager 43
operating systems 29
over-temperature 49

P

password
file reset 54
maintenance mode 53
restore default 54
peer 25
performance
device 20
switch 18
PKI - See Public Key Infrastructure
planning 17
policy
IKE 25
security 25
port
binding 26
buffer credits 18
characteristics 67
diagnostics 50
Ethernet 12
fabric 11
Fibre Channel 10
generic 11
LEDs 10
maximum number of ports/users 68
number of 67
security 26
serial 12
speed 68
transparent routing 11

types 11, 67
POST - See Power-on self test
power
consumption 69
requirements 30
source loading 69
Power-on self test
description 48
fatal error 48
principal
priority 21
switch 21
processor 29, 68
Public Key Infrastructure 25

Q

QuickTools
service 23
web applet 14

R

rack mount 31
rack stability, warning 58
RADIUS - See Remote Dial-In User Service.
recovering a switch 53
remake filesystem 54
Remote Dial-In User Service 25, 26
Remote Support Pack 43
Remote Support Software Manager 43
RS-232 port 12

S

scalability 67
Secure Shell
description 26
service 23
Secure Socket Layer service 23
security
association 25
certificate 26
connection 26
database limits 26
device 26
fabric 25
IP 25
policy 25
user account 25
serial port 12, 35, 37
SFP - See Small Form-Factor Pluggable
shock 70
Simple Mail Transfer Protocol 24
Simple Network Management Protocol
description 14
service 23
site requirements 29
small form-factor pluggable 11, 35
SMI-S - See Storage Management Initiative-Specification
SMTP - See Simple Mail Transfer Protocol
SNMP - See Simple Network Management Protocol
soft zone 17
SSH - See Secure Shell
SSL - See Secure Socket Layer
Storage Management Initiative-Specification 15
Subscriber's choice, HP 58
surface mount 31
switch
add to fabric 42
air flow 68
configuration 37
diagnostics 47
management 13
management service 23
power up 36
recovery 53
reset 9, 55
services 23
shock 70
specifications 67
upgrade 10
vibration 70
symbols in text 57
System Fault LED 8, 47
system processor 68

T

technical support, HP 58
Telnet service 23
temperature
error 49
operating range 30, 70
text symbols 57
timeout values 51
TR_Port 11
transceiver
description 11
diagnostics 52
installation 35
transmission rate 18, 19
transparent routing 11, 21

U

upgrade 10
user account security 25
user interface 68

V

vibration 70
voltage 69

W

warning, rack stability 58
web applet
description 14
service 23
websites
HP documentation 59

HP storage 59
HP Subscriber's choice 58
workstation
configuration 35
connecting 37
IP address 35
operating system 12
requirements 29

Z

zone
conflict 51
definition 17
zone set
active 17
definition 17
zoning
database 17
hardware-enforced 17
limits 17