QLOGIC®

The Ultimate in Performance

QLogic 9000 Series Stackable Chassis Switch

Installation Guide

Firmware Version 7.8

59229-05 A

Information furnished in this manual is believed to be accurate and reliable. However, QLogic assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic assumes no responsibility for any errors that may appear in this document.

This switch is covered by one or more of the following patents: 6697359; other patents pending.

Document Revision History	
Draft, Revision 1, September 8, 2009	Firmware Version 7.8 Enterprise Fabric Suite 2007 Version 7.08

Table of Contents

Preface

1 General Description

2 Planning

5 Customer Replaceable Units

A Specifications

List of Figures

List of Tables

Table **Page**

Preface

This manual describes the features and installation of the QLogic 9000 Series Stackable Chassis Switch, firmware version 7.8. This manual is organized as follows:

- This preface describes the intended audience, related materials, safety notices, communications statements, laser safety information, electrostatic discharge sensitivity precautions, accessible parts, general program license, and technical support.
- Section 1 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Section 2 describes the factors to consider when planning a fabric.
- Section 3 explains how to install and configure the switch.
- Section 4 describes the diagnostic methods and troubleshooting procedures.
- Section 5 describes the removal/replacement procedures for all customer replaceable units (CRU).
- Appendix A lists the switch specifications.

Please read the communications statements and laser safety information later in this section.

Intended Audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide*, publication number 59231-04
- *SANbox Fibre Channel Switch CLI Quick Reference Guide*, publication number 59261-03
- *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide*, publication number 59230-04.
- *SANbox 9000 Series QuickTools Switch Management User Guide*, publication number 59234-04
- *QLogic Fibre Channel Switch Event Message Guide*, publication number 59060-06
- *SANbox Simple Network Protocol Reference Guide*, publication number, 59047-09
- *CIM Agent Reference Guide*, publication number 59223-03
- *QLogic Switch Interoperability Guide v3.0*. This PDF document can be downloaded at http://www.qlogic.com/interoperability/interoperability.aspx.
- RFC 2865 *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2869 *RADIUS Extensions*
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

> Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
> Fax: (303) 397-2740.

Safety Notices

A **Warning** notice indicates the presence of a hazard that has the potential of causing personal injury.

3-5, 3-9, 3-13, 5-6, 5-16, 5-21

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

3-5, 3-12, 5-2, 5-4, 5-12, 5-13, 5-17, 5-21

Sicherheitshinweise

Ein **Warnhinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Verletzungen zur Folge hat.

3-5, 3-9, 3-14, 5-6, 5-16, 5-21

Ein **Vorsichtshinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Geräteschäden zur Folge hat.

3-6, 3-12, 5-2, 5-4, 5-12, 5-13, 5-17, 5-22

Notes informatives relatives à la sécurité

Une note informative **Avertissement** indique la présence d’un risque pouvant entraîner des blessures.

3-5, 3-9, 3-13, 5-6, 5-16, 5-21

Une note informative **Précaution** indique la présence d’un risque pouvant entraîner des dégâts matériels.

3-6, 3-12, 5-2, 5-4, 5-12, 5-13, 5-17, 5-22

Advertencias de seguridad

Un aviso de **Advertencia** indica la presencia de un peligro que puede causar lesiones personales.

3-5, 3-9, 3-14, 5-6, 5-16, 5-21

Un aviso de **Precaución** indica la presencia de un peligro que puede causar daño al equipo.

3-7, 3-12, 5-3, 5-4, 5-12, 5-13, 5-18, 5-22

Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

Federal Communications Commission (FCC) Class A Statement

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.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Class A Compliance Statement

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.

Avis de conformité aux normes du ministère des Communications du Canada

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.

CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (89/336/EEC) and to the Low Voltage (Safety) Directive (73/23/EEC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN60950-1, A11:2004 – “Safety of Information Technology Equipment, Including Electrical Business Equipment”.
- EN 55022:1998, A1:2000, A2:2003 – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN 55024:1998, A1:2001, A2:2003 – “Electromagnetic compatibility - Generic immunity standard Part 1: Residential commercial, and light industry.”
  - ❑ EN 61000-4-2: 1995, A1:1998, A2: 2001 – “Electrostatic Discharge Immunity Test”
  - ❑ EN 61000-4-3: 2002 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - ❑ EN 61000-4-4: 1995, A1:2001, A2:2001 – “Electrical Fast Transient/Burst Immunity Test”
  - ❑ EN 61000-4-5: 1995, A1:2001 – “Surge Immunity Test”
  - ❑ EN 61000-4-6: 1996, A1:2001 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - ❑ EN 61000-4-8: 1993, A1:2001 – "Power Frequency Magnetic Field Immunity Test”
  - ❑ EN 61000-4-11 Second Edition: 2004 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN 61000-3-2: 2000 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN 61000-3-3: 1995, A1:2001 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

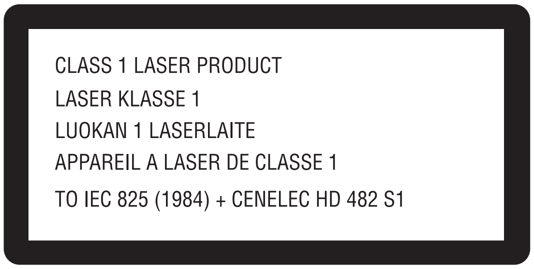
VCCI Class A Statement

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。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Laser Safety Information

This product may use 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.



CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1
TO IEC 825 (1984) + CENELEC HD 482 S1

Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

Accessible Parts

The Customer Replaceable Units (CRU) in the QLogic 9000 Series Stackable Chassis Switch are the following:

- Small Form-Factor Pluggable (SFP) optical transceivers
- X2 optical transceivers
- I/O blades
- CPU blades
- Power Supply blades
- Fan blades

Refer to Section 5 for more information.

Pièces Accessibles

Les pièces remplaçables, Customer Replaceable Units (CRU), du commutateur QLogic 9000 Series Stackable Chassis Switch sont les suivantes:

- Interfaces aux media d’interconnexion appelés SFP transceivers.
- Interfaces aux media d’interconnexion appelés X2 transceivers.
- Modules des entrée/sortie
- Modules des unite centrale
- Modules d'alimentation de courant
- Modules des Ventilateurs

Se reporter à la Section 5 (Procédures de retrait et remplacement) pour plus de renseignements.

Zugängliche Teile

Nur die folgenden Teile im QLogic 9000 Series Stackable Chassis Switch können kundenseitig ersetzt werden:

- Schnittstellen für die Zwischenverbindungsträger, SFP transceivers genannt.
- Schnittstellen für die Zwischenverbindungsträger, X2 transceivers genannt.
- Blätter Des Einganges/Ausganges
- Zentraleinheitsmodules
- Netzteilmodules
- Gehäuselüftemodules

Weitere Informationen finden Sie im Abshcnitt 5 (Ausbauen der ersetzbaren Teile).

License Agreements

Refer to the *QLogic Software End User License Agreement* for a complete listing of all license agreements affecting this product.

New in this Release

This release includes the following new features:

- Support for the 8-Gbps I/O blade
- Support for Internet Protocol version 6
- Support for Internet Protocol Security
- Support for Simple Network Management Protocol version 3 user accounts
- Support for the Tech_Support_Center Call Home profile. This profile provides for the automatic capture and communication of switch status and trend data periodically by e-mail to specified technical support resources.

Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support web site listed in Contact Information for the latest firmware and software updates.

Availability

QLogic Technical Support for products under warranty is available during local standard working hours excluding QLogic Observed Holidays.

Training

QLogic offers training for technical professionals for all iSCSI, InfiniBand, and Fibre Channel products. From the main QLogic web page at www.qlogic.com, click the **Education and Resources** tab at the top, then click the **Education & Training** tab on the left. The QLogic Global Training Portal offers online courses, certification exams, and scheduling of in-person training.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by e-mail at training@qlogic.com.

Contact Information

Please feel free to contact your QLogic approved reseller or QLogic Technical Support at any phase of integration for assistance. QLogic Technical Support can be reached by the following methods:

Web	http://support.qlogic.com
Email	support@qlogic.com

The QLogic knowledge database contains troubleshooting information for the QLogic adapters. Access the data base from the QLogic Support web page, http://support.qlogic.com. Use the Support Center search engine to look for specific troubleshooting information.

Notes

1 General Description

This section describes the features and capabilities of the QLogic 9000 Series Stackable Chassis Switch. The following topics are described:

- Hardware Overview
- Maintenance Panel
- I/O Blades
- CPU Blades
- Power Supply Blades
- Fan Blades
- Fabric and Switch Management

Hardware Overview

The QLogic 9000 Series switch is set of up to eight I/O blades interconnected with all other I/O blades through the midplane. One or two CPU blades provide configuration, monitoring, data path management, and control functions. Dual Power Supply blades provide power, and dual Fan blades provide cooling.

Table 1-1 describes the available models.

Table 1-1. QLogic 9000 Series Switch Models

Model Number	I/O Blades	CPU Blades	Power Supply Blades	Fan Blades
9100	0	1	2	2
9200	0	2	2	2

I/O blades are ordered separately so that you can specify how many I/O blades you want and what types. To maintain proper air flow and cooling, blank panels are installed in empty I/O slots. The following I/O blade types are available:

- 16-port 4-Gbps I/O blade
- 16-port 8-Gbps I/O blade
- 4-port 10-Gbps I/O blade

Figure 1-1 shows a QLogic Model 9200 switch, two I/O blades, and the corresponding blade IDs.

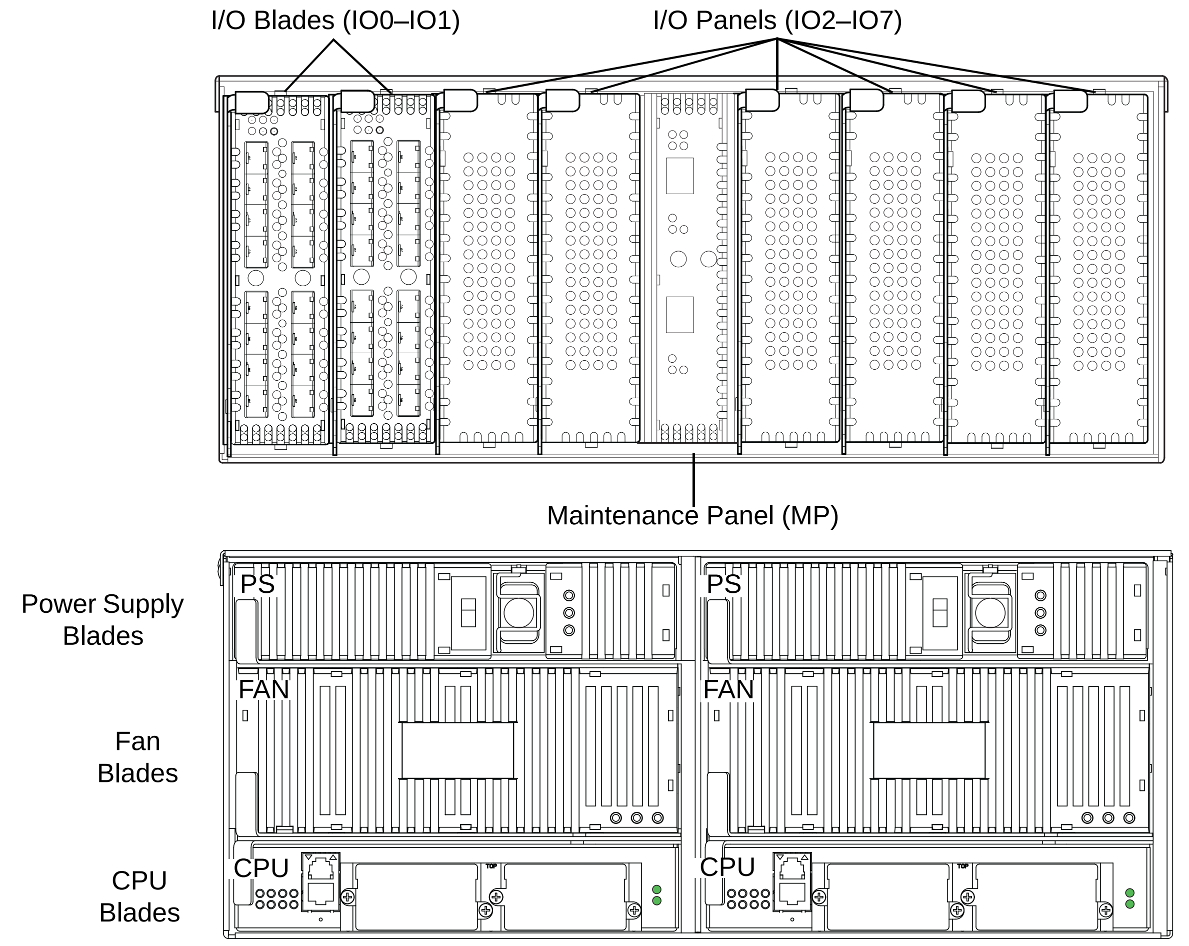


Figure 1-1 QLogic 9000 Series Switch Model Components

I/O blades (IO0–IO7), CPU blades (CPU0, CPU1), Power Supply blades (PS0, PS1), and the Fan blades (FAN0, FAN1) are identified based on where they are installed in the chassis. The Maintenance Panel (MP) is not removable and provides switch status and alternate access to the CPU blade LEDs and Ethernet ports.

Maintenance Panel

The Maintenance Panel provides a status interface for the switch and alternate Ethernet ports for the two CPU blades as shown in Figure 1-2. The chassis LEDs are as follows:

- Chassis Good LED (Green)–This LED illuminates to indicate that switch is operational. This means that the primary CPU (CPU0) is functioning.
- Chassis Power LED (Green)–This LED illuminates to indicate that at least one CPU blade is receiving power.
- Chassis Beacon LED (White)–This LED and all other Beacon LEDs illuminate in response to a command issued from the management workstation to help locate a switch.
- Chassis Fault LED (Amber)–This LED illuminates to indicate that a fatal error has occurred on one or more of the I/O blades, CPU, Power Supply, or Fan blades.

The CPU blade LEDs are described in “CPU Blades” on page 1-9.

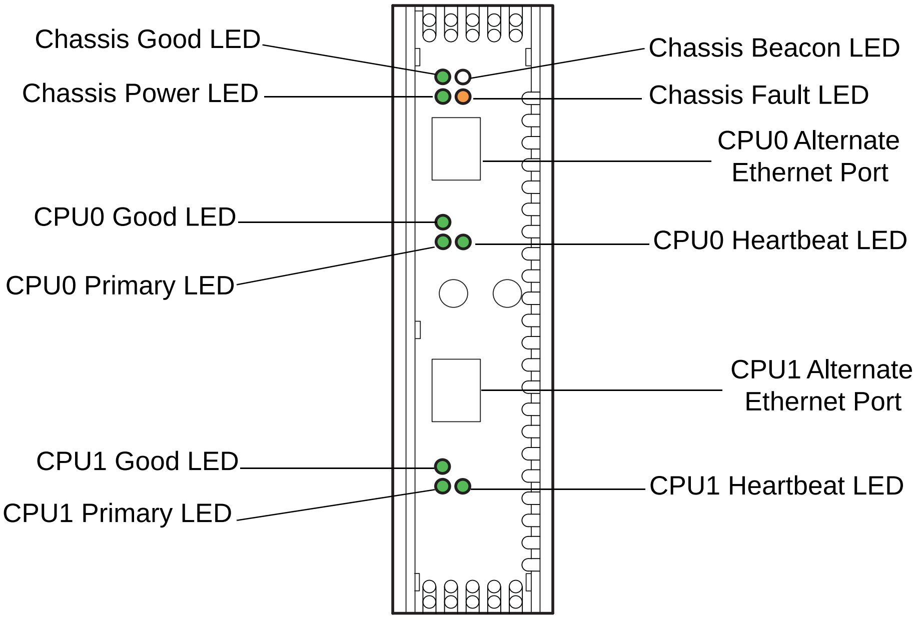


Figure 1-2 Maintenance Panel

Initially, the alternate Ethernet ports are inactive, thus requiring that you make the Ethernet connection on the primary CPU blade. You can activate the alternate primary Ethernet port on the Maintenance Panel using QuickTools, Enterprise Fabric Suite 2007, or the CLI.

NOTE:

> You can activate both Maintenance Panel Ethernet ports or both CPU blade Ethernet ports by installing the Fault Tolerant license key. Refer to "Installing Feature License Keys" on page 3-28.

I/O Blades

The I/O blades transmit and receive I/O traffic. There are three types of I/O blades:

- A 4-Gbps I/O blade has 16 Small Form-factor Pluggable (SFP+) ports and is capable of 4-, 2-, or 1-Gbps transmission.
- The optional 8-Gbps I/O blade has 16 SFP+ ports and is capable of 8-, 4-, or 2-Gbps transmission.
- A 10-Gbps I/O blade has four X2 ports and is capable of 10-Gbps transmission. 10-Gbps I/O blades are used to connect to a QLogic 5000 series switch using an X2-XPAK stacking cable, or to another QLogic 9000 Series switch using an X2-X2 stacking cable.

An I/O blade slot is known by its blade ID and is configured with a blade type. The I/O blade IDs are a composite of the IO descriptor and slot number. For example, the blade ID for an I/O blade in slot 0 would be IO0 and so on through IO7.

The blade type is the operating characteristic of the I/O slot that defines the supported protocol, transmission speed, and number of ports. The switch automatically configures the I/O slot blade type based on the installed I/O blade. The following blade types are supported:

- FC8G16–Fibre Channel 8/4/2-Gbps I/O blade
- FC4G16–Fibre Channel 4/2-Gbps I/O blade
- FC10G4–Fibre Channel 10-Gbps I/O blade.

Fibre Channel ports are numbered based on the blade ID as shown in Figure 1-3. For example, for I/O blade IO0 with blade type FC8G16 or FC4G16, ports are always numbered 0–15. IO1 ports would be numbered 16–31, and so on up to a maximum of 127. For I/O blade IO0 with blade type FC10G4, ports are always numbered 0–3. FC ports can also be identified by I/O blade and port number. For example, port 0 is also known as IO0-0. The ports configure themselves to communicate with devices and other switches.

Each I/O blade features a set of LEDs, Fibre Channel (FC) ports, and FC port LEDs as shown in Figure 1-3.

- I/O Blade LEDs
- FC Port LEDs
- Port Types
- Transceivers and 10-Gbps Stacking Cables

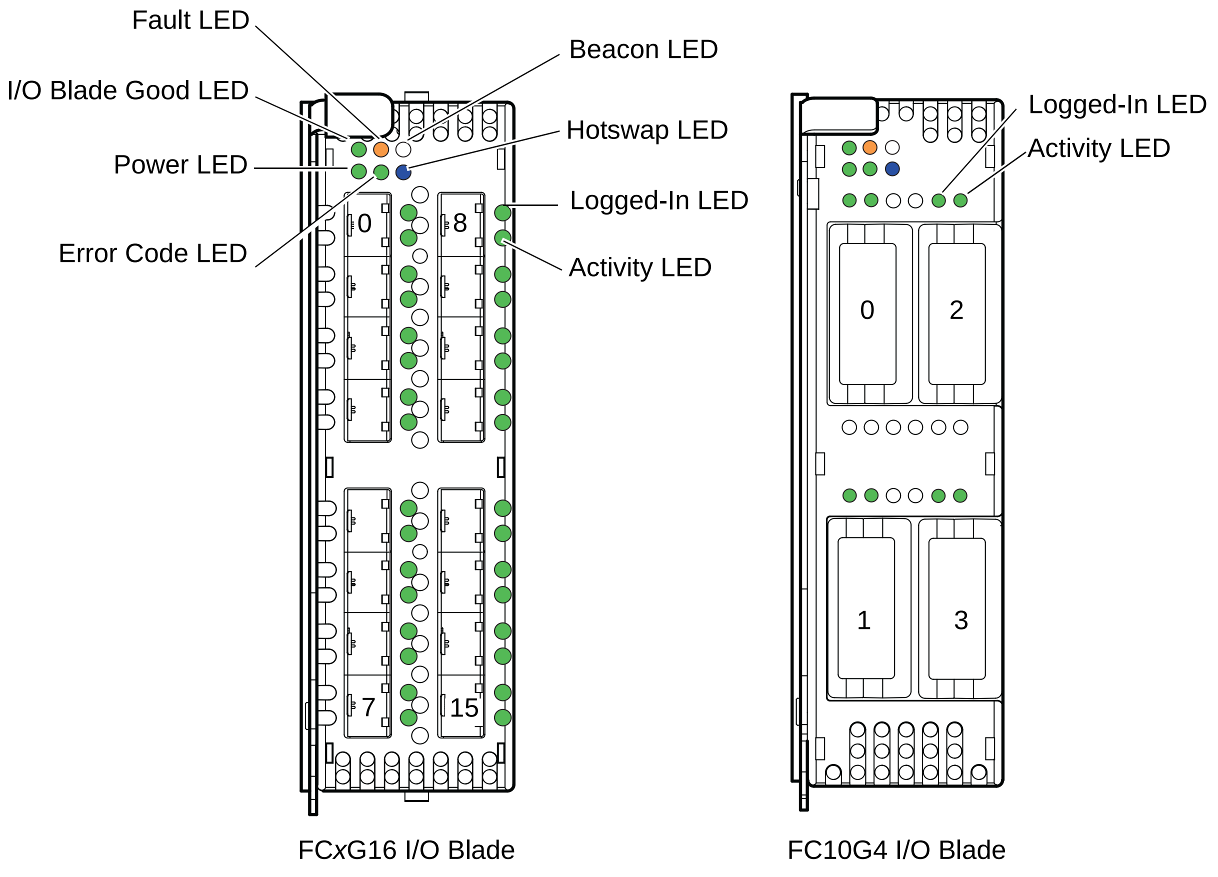


Figure 1-3 I/O Blades

I/O Blade LEDs

The I/O blade LEDs are as follows:

- I/O Blade Good LED (Green)–This LED illuminates to indicate that the I/O blade is operational.
- I/O Blade Power LED (Green)–This LED illuminates to indicate that the I/O blade is receiving power.
- I/O Blade Fault LED (Amber)–This LED illuminates to indicate that the I/O blade has a fatal error. This LED and the Chassis Fault LED illuminate together.
- I/O Blade Error Code LED (Green)–This LED is reserved for future use.
- I/O Blade Beacon LED (White)–This LED illuminates in response to a command issued from the management workstation to help locate an I/O blade.
- I/O Blade Hotswap LED (Blue)–This LED illuminates to indicate the I/O blade insertion status. Continuous illumination indicates that the I/O blade is not fully seated.

FC Port LEDs

The FC Port LEDs are as follows:

- Logged-in LED (Green)–This LED illuminates to indicate 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 initialization or 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 will extinguish. Refer to "FC Port Diagnostics" on page 4-8 for more information about the Logged-In LED.
- Activity LED (Green)–This LED illuminates to indicate that data is passing through the port. Each frame that the port transmits or receives causes this LED to illuminate for 50 milliseconds. This makes it possible to observe the transmission of a single frame. When extending credits, the Activity LED for a donor port will reflect the traffic of the recipient port. Refer to "Distance" on page 2-3 for more information about extended credits and donor ports.

Port Types

The switch supports generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), and expansion ports (E_Port). Switches come from the factory with all ports configured as GL_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a public loop device, as an F_Port when connected to a single public 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.
- A G_Port self-configures as an F_Port when connected to a single public device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 public devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single public device (N_Port).
- An F_Port supports a single public device. F_Ports also support N_Port ID Virtualization (NPIV).

E_Ports enable you to expand the fabric by connecting QLogic 9000 Series switches with other switches. QLogic 9000 Series switches self-discover all inter-switch connections. Refer to “Multiple Chassis Fabrics” on page 2-6 for more information about multiple chassis fabrics.

Transceivers and 10-Gbps Stacking Cables

SFP and X2 transceivers convert electrical signals to and from optical laser signals to transmit and receive. SFP transceivers plug into the SFP ports; X2 transceivers plug into the X2 ports. Duplex fiber optic cables plug into the transceivers, which then connect to the devices. An SFP port is capable of transmitting at 8-Gbps, 4-Gbps, 2-Gbps, or 1-Gbps depending on the I/O blade type; however, the transceiver must be capable of delivering at the desired rate. 10-Gbps ports transmit at 12.75-Gbps.

SFP and X2 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. Refer to “Replacing Transceivers and Stacking Cables” on page 5-3 for information about installing and removing transceivers.

10-Gbps stacking cables are available to connect the QLogic 9000 Series switch to other QLogic switches using the X2 ports.

- An X2-XPAK stacking cable connects a QLogic 9000 Series switch and a QLogic 5000 series switch.
- An X2-X2 stacking cable connects two QLogic 9000 Series switches. Refer to “HyperStacking” on page 3-29 for information about connecting QLogic 9000 Series switches through the high bandwidth Inter-Chassis connectors.

CPU Blades

The CPU blade, shown in Figure 1-4, provides configuration, monitoring, data path management, and control functions. The switch has two CPU blades which are identified by their blade IDs: CPU0 and CPU1.Initially, CPU0 is the primary CPU blade and controls all management functions. CPU1 is the secondary CPU blade and provides redundant interconnections for all ports through the switch midplane. Without the Fault Tolerant license key, the only way that the CPU1 blade can assume management control is by removing the CPU0 blade before powering up the switch.

NOTE:

> The Fault Tolerant license key provides for automatic and manual transfer of switch management functions from the primary CPU blade to the secondary CPU blade for switches equipped with two CPU blades. Refer to "Installing Feature License Keys" on page 3-28 for information about installing license keys.

Each CPU blade has the following components:

- CPU Blade LEDs
- Maintenance Button
- Ethernet Port
- Inter-Chassis Connection Ports

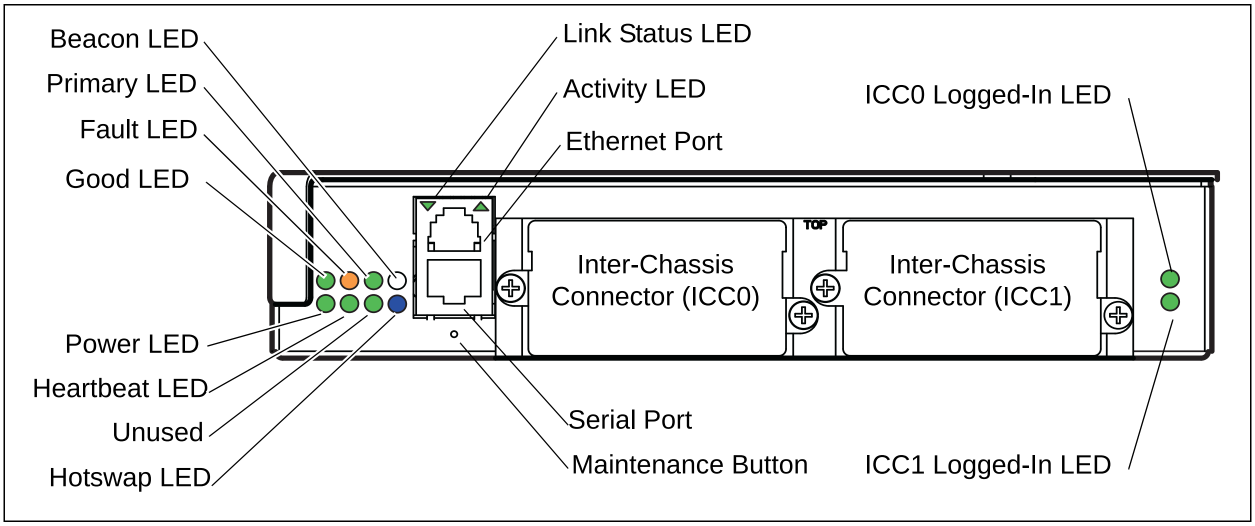


Figure 1-4 CPU Blade

CPU Blade LEDs

The CPU blade LEDs indicated the operating condition of the CPU blade. The CPU Good LED, CPU Heartbeat LED, and CPU Primary LED are replicated on the Maintenance Panel. The CPU blade LEDs are as follows:

- CPU Good LED (Green)–This LED illuminates to indicate that the CPU blade is operational. In maintenance mode, this LED is off.
- CPU Fault LED (Amber)–This LED illuminates to indicate that the CPU blade has a fatal error. This LED and the Chassis Fault LED illuminate together.
- CPU Primary LED (Green)–This LED illuminates to indicate the primary CPU.
- CPU Beacon LED (White)–This LED illuminates in response to a command issued from the management workstation to help locate a CPU blade.
- CPU Power LED (Green)–This LED illuminates to indicate that the CPU blade is receiving power.
- CPU Heartbeat LED (Green)–This LED indicates the status of the CPU internal switch processor and the results of the Power On Self Test (POST). During normal operation, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. Certain errors will cause the Heartbeat LED to blink an error code. Refer to “Error Code Blink Patterns” on page 4-2 for error code explanations. In maintenance mode, the Heartbeat LED illuminates continuously.
- CPU Hotswap LED (Blue)–This LED illuminates to indicate the CPU blade insertion status. Continuous illumination indicates that I/O traffic has ceased and the CPU blade can be removed.

Maintenance Button

The Maintenance button is a dual-function momentary switch on the CPU blade. Its purpose is to reset a CPU blade or to place the switch in maintenance mode. Maintenance mode is used to recover the switch when flash memory or the resident configuration file is corrupted. Refer to "Recovering a Switch Using Maintenance Mode" on page 4-15 for more information about using maintenance mode.

Resetting a CPU Blade

To reset a CPU blade, use a pointed tool to momentarily press and release the Maintenance button on a CPU blade.

Placing the Switch in Maintenance Mode

Maintenance mode removes power from the I/O blades, and temporarily sets the switch IP address to 10.0.0.1. To place the switch in maintenance mode, isolate the switch from the fabric, then do one of the following:

- For a single CPU blade switch:
    1. Using a pointed tool, press and hold the Maintenance button.
    2. When the CPU blade Heartbeat LED illuminates steady, release the Maintenance button.
- For a dual CPU blade switch:
    1. If there are two Ethernet connections, disconnect one of them.
    2. Power down the switch.
    3. Power up the switch. As the switch is powering up, using two pointed tools, press and hold the Maintenance buttons on both CPU blades at approximately the same time. When the CPU blade Heartbeat LED illuminates steady, release the Maintenance buttons.

To exit maintenance mode and return to normal operation, do the following:

- For a single CPU blade switch, momentarily press and release the Maintenance button, or power cycle the switch.
- For a dual CPU blade switch, power cycle the switch.

Ethernet Port

Each CPU blade has an Ethernet port and a serial port.The Ethernet port is an RJ-45 connector that provides a connection to a management workstation through a 10/100 Base-T Ethernet cable. The Ethernet port automatically recognizes straight or cross-over cables. The default IP address for the CPU0 Ethernet port is 10.0.0.1. Initially, only the CPU0 blade Ethernet port is active.

NOTE:

If the Fault Tolerant license key is installed, the Ethernet ports on both CPU blades are active. However, all communication is routed through the primary CPU blade Ethernet port.

A management workstation can be a Windows®, Solaris™, Linux®, or MacOS X® workstation that is used to configure and manage the switch fabric. You can manage the switch over an Ethernet connection using QuickTools™, the Command Line Interface (CLI), Enterprise Fabric Suite 2007, or SNMP. The switch through which the fabric is managed is called the fabric management switch.

There are alternate Ethernet ports on the Maintenance panel for each CPU blade that are initially inactive. You can activate the primary CPU Ethernet port on the Maintenance panel instead of the Ethernet port on the CPU blade using the Set Setup System CLI command, QuickTools, or Enterprise Fabric Suite 2007. If the Fault Tolerant license key is installed, you can choose to activate both CPU blade Ethernet ports or both Maintenance Panel Ethernet ports, but not all four.

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (amber). 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.

Serial Port

The serial port is an RJ-45 connector and uses a 10/100 Base-T Ethernet straight cable with the RJ-45/RS-232 console adapter provided with the switch. You manage the switch through the primary CPU blade serial port using the CLI.

Inter-Chassis Connection Ports

NOTE:

You can activate the Inter-Chassis Connection ports by installing the HyperStack license key. Refer to "HyperStacking" on page 3-29 for information about HyperStacking switches.

Each CPU has two Inter-Chassis Connection (ICC0, ICC1) ports with which to establish a connection with another QLogic 9000 Series switch. Each ICC port is a bundle of eight 10-Gbps Fibre Channel ports that log in to a second QLogic 9000 Series switch. The ICC port Logged-In LEDs show the ICC port connection status.

Power Supply Blades

The Power Supply blades convert standard 100 to 240 VAC to DC voltages for the various switch circuits. After connecting a power supply to an AC voltage source and placing the On/Off switch in the On position, the Power Supply blade is energized. During normal operation, each Power Supply blade provides half of the demand. If one Power Supply blade fails, the second Power Supply blade can provide all of the switch power needs for a short time until the failed Power Supply blade can be replaced. Refer to "Replacing Power Supply Blades" on page 5-16 for more information.

Power Supply blades are known to the switch firmware by their blade IDs and blade types. The blade IDs (PS0, PS1) indicate the blade type and location in the switch chassis. The blade types (PSFB, PSBF) indicate the blade type and air flow direction. Air flow direction can be front-to-back or back-to-front. In addition to the blade ID, a label on the body of the Power Supply blade indicates the air flow direction.

CAUTION!

To prevent overheating and damage to switch circuits, Power Supply and Fan blades must have the same air flow direction. The System Fault LED will illuminate if the Power Supply and Fan blades do not have the same air flow direction.

Each Power Supply blade has an AC power receptacle, an On/Off switch, and a set of LEDs as shown in Figure 1-5. The Power Supply blade LEDs are as follows:

- Power Supply Power LED (Green)–This LED illuminates to indicate that the Power Supply blade is operational.
- Power Supply Fault LED (Amber)–This LED illuminates to indicate that the Power Supply blade has a fault. This LED and the Chassis Fault LED illuminate together.
- Power Supply Beacon LED (White)–This LED illuminates in response a command issued from the management workstation to help locate a Power Supply blade.

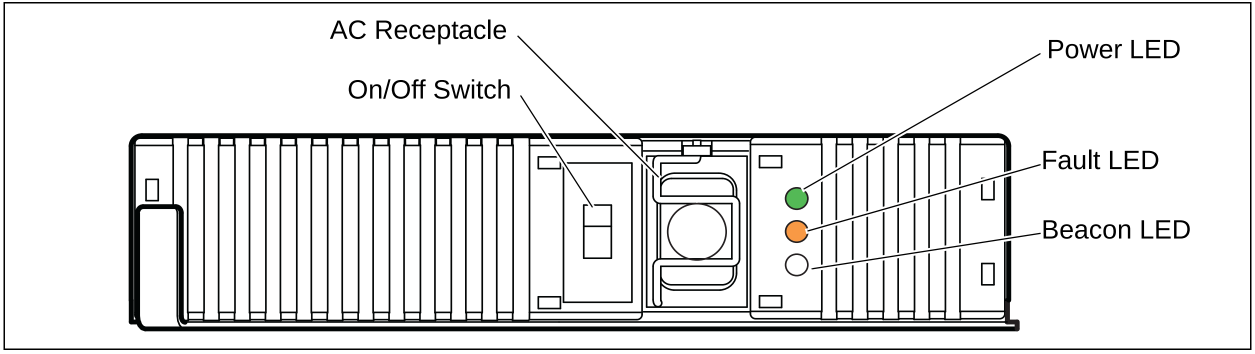


Figure 1-5 Power Supply Blade

Fan Blades

The switch is equipped with two Fan blades that cool the switch. Both Fan blades must be installed and operational to provide adequate cooling for the switch. The Fan blades are hot pluggable and interchangeable. Refer to "Replacing Fan Blades" on page 5-21 for information about removing and installing Fan blades.

Fan blades are known by their blade IDs and blade type. The blade IDs (FAN0, FAN1) indicate the blade type and location in the switch chassis. The blade type (FANFB, FANBF) indicate the blade type and air flow direction. Air flow direction can be front-to-back or back-to-front. In addition to the blade ID, a label on the body of the Fan blade indicates the air flow direction.

CAUTION!

> To prevent overheating and damage to switch circuits, Power Supply and Fan blades must have the same air flow direction. The System Fault LED will illuminate if the Power Supply and Fan blades do not have the same air flow direction.

Each Fan blade has a set of LEDs as shown in Figure 1-6, that indicate the Fan blade operational status. The Fan blade LEDs are as follows:

- Fan Power LED (Green)–This LED illuminates to indicate that the Fan blade is receiving power.
- Fan Fault LED (Amber)–This LED illuminates to indicate that the Fan blade has a fault. This LED and the Chassis Fault LED illuminate together.
- Fan Beacon LED (White)–This LED illuminates in response to a command issued from the management workstation to help locate a Fan blade.

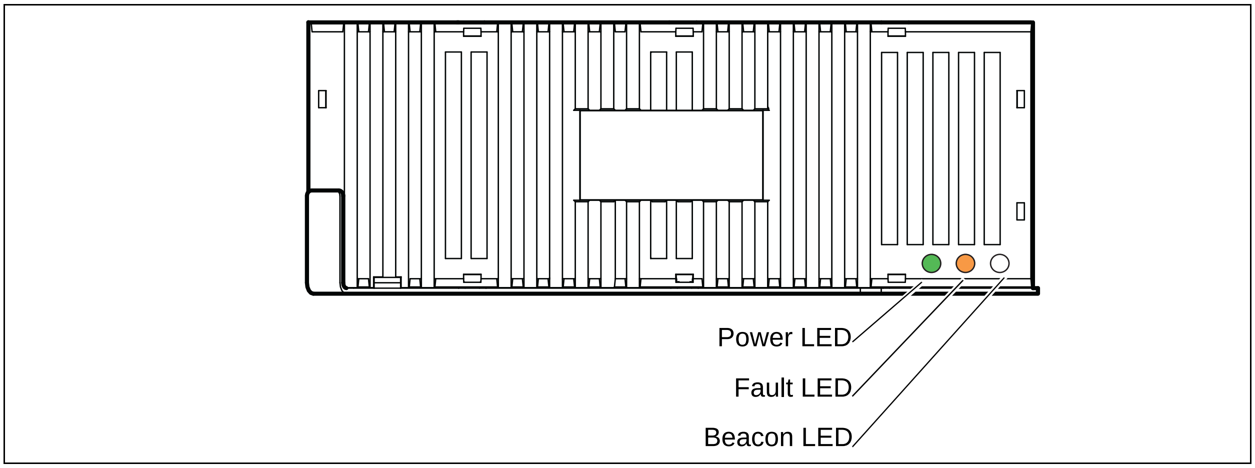


Figure 1-6 Fan Blade

Fabric and Switch Management

The switch supports the following management tools:

- Enterprise Fabric Suite 2007
- QuickTools
- Command Line Interface
- Application Programming Interface
- Simple Network Management Protocol
- Storage Management Initiative–Specification (SMI-S)
- File Transfer Protocols

Enterprise Fabric Suite 2007

Enterprise Fabric Suite 2007 is a workstation-based Java® application that provides a graphical user interface for fabric management. This includes Performance View which graphs port performance. Enterprise Fabric Suite 2007 can run on a Windows, MacOS, Solaris, or Linux workstation. A management workstation connects to the fabric through the Ethernet port of one or more switches and can provide in-band management for all other switches in the fabric. Refer to the *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide* for information about the Enterprise Fabric Suite 2007 application and its use.

QuickTools

To provide basic fabric management tools in a graphical user interface and to make switch management less dependent on a particular platform, each switch contains an web applet called QuickTools. You run QuickTools by opening the switch IP address with an internet browser. You will be prompted to install the Java 2 Standard Edition Runtime Environment application if it is not already installed on your workstation.

QuickTools performs the following basic switch management tasks:

- Monitor fabric and switch status
- Display device information
- Manage device nicknames
- Enable or disable SNMP
- Enable or disable in-band management
- Managing zoning
- Manage user accounts
- Display switch information
- Configure switches
- Reset a switch
- Install firmware
- Display port information
- Configure ports
- Extend port buffer credits
- Reset a port
- Test a port

Refer to the *SANbox 9000 Series QuickTools Switch Management User Guide* for more information.

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. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for more information.

Application Programming Interface

The Application Programming Interface (API) enables an application provider to build a management application for QLogic switches. The library is implemented in ANSI standard C, relying only on standard POSIX run-time libraries (except for the Windows NT build). Contact your distributor or authorized reseller for information about the API.

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. 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. The default configuration enables SNMP.

SNMP version 3 provides secure access to devices through a combination of authentication and encryption. The default configuration disables SNMP version 3 security.

You can enable SNMP, configure SNMP traps, and configure SNMP version 3 security using Enterprise Fabric Suite 2007, QuickTools, or the CLI. Refer to the *SANbox Simple Network Management Protocol Reference Guide* for information about using SNMP.

Storage Management Initiative–Specification (SMI-S)

SMI-S Provides for the management of the switch through third-party applications that use the SMI-S. Refer to the *CIM Agent Reference Guide* for more information.

File Transfer Protocols

File transfer between the switch and the management workstation is available using the File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

2 Planning

Consider the following when planning a fabric:

- Devices
- Device Access
- Performance
- Feature Licensing
- Multiple Chassis Fabrics
- Switch Services
- Internet Protocol Support
- Security
- Fabric Management

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 the number of switches.
- The transmission speeds of your HBAs and SFPs. The SFP ports support 1-Gbps, 2-Gbps, and 4-Gbps transmission speeds depending on the SFP. 8-Gbps I/O blades also support 8-Gbps.

NOTE:

Setting an SFP port to 1-Gbps that has an 8-Gbps SFP transceiver will down the port.

- The distribution of target and initiator devices. 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 zones and zone sets. Some zoning strategies include the following:

- Separate devices by operating system
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate 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 2-1 describes the zoning database limits, excluding the active zone set.

Table 2-1. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256).
MaxZones	Maximum number of zones (2000) including orphan zones
MaxAliases	Maximum number of aliases (2500).
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch 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 (2000), excluding the orphan zone set. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

Performance

The QLogic 9000 Series switch supports class 2 and class 3 Fibre Channel service at transmission rates of 1-, 2-, 4-, 8-, and 10-Gbps with a maximum frame size of 2148 bytes. A port adapts its transmission speed to match that of the device to which it is connected prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

Distance

Consider the physical distribution of devices and switches in the fabric. Choose transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Appendix A for more information about cable types and transceivers.

Each SFP and X2 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 the following approximate distances:

- 26 kilometers at 1-Gbps (0.6 credits/Km)
- 13 kilometers at 2-Gbps (1.2 credits/Km)
- 6 kilometers at 4-Gbps (2.4 credits/km)
- 3 kilometers at 8-Gbps (4.8 credits/km)
- 2 kilometers at 10-Gbps (7.2 credits/km)

Longer distances can be spanned at full bandwidth on SFP ports and X2 ports by extending credits to G_Ports, F_Ports, and E_Ports using Enterprise Fabric Suite 2007. Each port can donate 15 credits to a pool from which a recipient port on the same I/O blade can borrow. The recipient port also loses a credit in the process. For example, you can configure a recipient port to borrow 15 credits from one donor port for a total of 30 credits (15+15=30).

Ports can borrow credits from other ports of like kind: SFP ports can borrow from SFP ports; X2 ports can borrow from X2. However, SFP ports cannot loan or borrow credits from X2 ports.

Regardless of how many credits are borrowed, extending credits requires a minimum cable length that is dependent on transmission speed. Extending credits over short cables can result in excessive port resets. Table 2-2 describes the distances that are possible for a port with 30 credits and the minimum cable lengths.

Table 2-2. Extended Credit Distances and Cable Lengths

Transmission Speed	Range for 30 Credits	Minimum Cable Length
1-Gbps	50 Km (30÷0.6)	3 Km
2-Gbps	25 Km (30÷1.2)	1.5 Km
4-Gbps	12 Km (30÷2.4)	750 m
8-Gbps	6 Km (30÷4.8)	370 m
10-Gbps	4 Km (30÷7.2)	250 m

Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. An SFP port can transmit or receive at nominal rates of 1-, 2-, 4-, or 8-Gbps depending on the device to which it is connected. This corresponds to full duplex bandwidth values of 212 MB, 424 MB, 850 MB, and 1700 MB respectively. X2 ports transmit at a nominal rate of 10-Gbps, which corresponds to a full-duplex bandwidth value of 2550 MB.

For optimal performance, devices connected to the same I/O blade should have the same transmission speed. Connecting devices of different transmission speeds on the same I/O blade can reduce the maximum bandwidth by as much as 10%.

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 2-Gbps source ports can transmit to one 4-Gbps 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.

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 between chassis.

Latency

Latency is a measure of how fast a frame travels from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship as shown in Table 2-3.

Table 2-3. Port-to-Port Latency

	Destination Rate				
	Gbps	2	4	8	10
Source Rate	2	< 0.4 µsec	< 0.4 µsec[a]	< 0.6 µsec[1]	< 0.4 µsec[1]
	4	< 0.3 µsec	< 0.3 µsec	< 0.4 µsec[1]	< 0.3 µsec[1]
	8	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec[1]
	10	< 0.3 µsec	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec

[a] Based on minimum frame size of 36 bytes. Latency increases for larger frame sizes.

Feature Licensing

License keys provide a way to expand the capabilities of your switch and fabric as your needs grow. Consider your need for the following features and make arrangements to purchase license keys from your switch distributor or authorized reseller.

- SANdoctor® provides access to the following tools:
  - ❑ Fibre Channel connection verification (Fcping CLI command)
  - ❑ Fibre Channel route tracing (Fctrace CLI command)
  - ❑ Transceiver diagnostic information (Show Media CLI command).
- HyperStacking enables you to connect two QLogic 9000 Series switches through the multiple 10-Gbps Inter-Chassis Connectors (ICC) allowing for up to 256 SFP ports.
- Fault Tolerance provides for automatic and manual failover of switch management functions from the primary CPU blade to the secondary CPU blade for switches equipped with two CPU blades.

Upgrading a switch is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller. Refer to “Installing Feature License Keys” on page 3-28 for information about installing license keys.

Multiple Chassis Fabrics

By connecting switches together 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 the QLogic 9000 Series switch with other switches in a wide variety of topologies.

- Optimizing Device Performance
- Domain ID, Principal Priority, and Domain ID Lock
- Interconnecting QLogic 9000 Series Switches

Optimizing Device Performance

When choosing a topology for a multiple chassis fabric, you should also consider the locality 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 QLogic 9000 Series switch provides the lowest latency of any product in its class. Refer to "Performance" on page 2-3 for information about latency and bandwidth. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single I/O blade. Therefore, for optimal device performance place devices on the same I/O blade 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-Gbps server and a slower 4-Gbps storage device
  - ❑ A high performance server and slow tape storage device

When planning a fabric, consider how to create redundant paths and minimize latency. Initiators and targets experience the least amount of latency when connected to the same I/O blade. For example, connecting initiators and targets ports together in parallel on two I/O blades, as shown in Figure 2-1, creates redundant paths and minimizes latency.

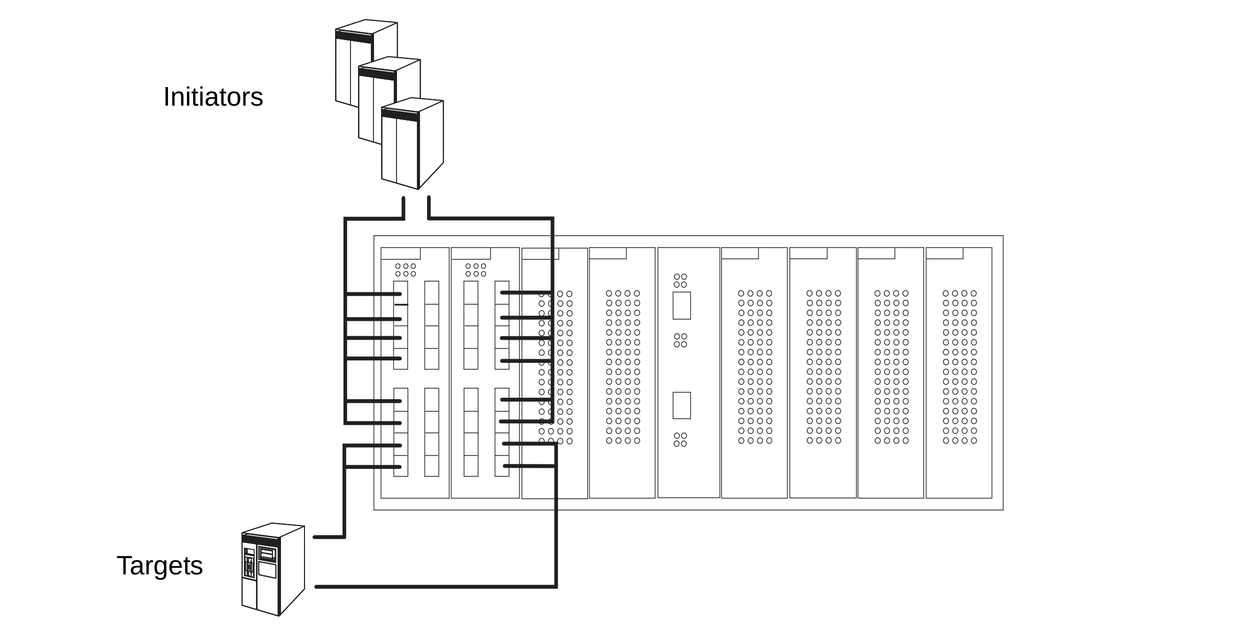


Figure 2-1 Single Switch Fabric with Initiators and Targets

Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis 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 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. Refer to the Set Config Switch command in the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about changing the default domain ID, domain ID lock, and principal priority parameters.

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. However, 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.

Interconnecting QLogic 9000 Series Switches

There are three ways to interconnect QLogic 9000 Series switches. The method you choose depends on your port count and bandwidth needs:

- SFP port-to-SFP port
- X2 port-to-X2 port
- ICC port-to-ICC port

An SFP-port connection provides up to 1700 MB of full duplex bandwidth for a FC8G16 I/O blade, while sacrificing an SFP port that would otherwise be available for devices.

An X2-port connection is established using an X2-X2 stacking cable. A 10-Gbps I/O blade is required in each switch. A 10-Gbps connection provides 2550 MB of full duplex bandwidth while preserving the SFP ports for devices. Refer to "Install Transceivers" on page 3-12 for more information.

ICC port connections require the HyperStacking license key on both switches and four HyperStacking cables. Each HyperStacking cable consists of eight 10-Gbps links connecting a CPU blade on one switch to a CPU blade on the second switch. This provides a total of 81.6 GB of full duplex bandwidth while preserving the I/O blade ports for devices. Refer to "HyperStacking" on page 3-29 for more information.

NOTE:

> If you connect two QLogic 9000 Series switches that have the same domain ID, the switches will isolate–there is no automatic domain ID conflict resolution. You must explicitly change the domain ID on one of the switches.

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 Enterprise Fabric Suite 2007, QuickTools, the Application Programming Interface (API), 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 Enterprise Fabric Suite 2007, QuickTools, SNMP, management server, or the API. 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 Enterprise Fabric Suite 2007, the QuickTools web applet, the API, and SMI-S. This service must be enabled to authenticate users through a RADIUS server when using Enterprise Fabric Suite 2007. To enable secure SSL connections, you must first synchronize the date and time on the switch and 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 is enabled.
- **Network Time Protocol (NTP)**: Provides for the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is disabled.

- **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)**: Provides for the management of the switch through third-party applications that use GS-3 Management Server. The default is enabled.
- **Call Home:** Provides for automated email notification of switch status and operating conditions based on specified event severity levels. The Call Home service is enabled by default. 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 email recipients, message format, and the event severity level that will initiate a message.

  Furthermore, you can configure periodic event data collection and processing through the Tech_Support_Center profile for automated status and trend analysis. With the purchase of a Prime Service contract, you may designate QLogic Technical Support to receive these notifications, in which case, QLogic will contact you proactively with recommended corrective actions whenever component failures or potential system problems are detected. Contact support@qlogic.com (1+952-932-4040) for assistance with the setup process and to determine the appropriate level of monitoring required.

Internet Protocol Support

The switch supports IP version 4, IP version 6, and Domain Name System (DNS) host names. IP versions 4 and 6 are enabled by default. Consider your IP version requirements and the availability of a DNS server.

Security

Security is available at the following levels:

- User Account Security
- Connection Security
- Port Binding
- Device Security

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, and Enterprise Fabric Suite 2007. 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. The default Admin account password is *password*. This password should be changed to ensure security. 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. Refer to "Connection Security" on page 2-13 for information about securing the management connection. A RADIUS server can also be used to authenticate devices and other switches as described in "Device Security" on page 2-14.

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.

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 IP version 4 and IP version 6 communications through the use of security policies and associations. Policies can define security for host-to-host, host-to-gateway, and gateway-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 to apply when called by a security policy. A security policy may call several associations at different times, but each association is related to only one policy. Consider your IP security requirements.

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. For information about port binding, refer to the *SANbox 9000 Series Stackable Chassis 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 Enterprise Fabric Suite 2007 and SMI-S.

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 command. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about the Create Certificate CLI command.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as Enterprise Fabric Suite 2007 (SSL), or both. Access to the device security menu selections in Enterprise Fabric Suite 2007 requires an SSL connection. 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.

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). ISL groups can be enabled for fabric binding. Fabric binding defines a list of switch domain IDs that are permitted to join the fabric.

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 1000.
- Maximum total number of group members is 1000.

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 Remote Authentication Dial-In User Service (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” on page 2-12. A secure connection is required to authenticate user logins with a RADIUS server. Refer to “Connection Security” on page 2-13 for more information.

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.

The following examples illustrate how to configure a security database:

- Security Example: Switches and HBAs with Authentication
- Security Example: RADIUS Server
- Security Example: Host Authentication

Security Example: Switches and HBAs with Authentication

Consider the fabric shown in Figure 2-2. In this fabric, Switch_1, HBA_1, and Switch_2 support authentication while the JBOD and HBA_2 do not. The objective is to secure F_Ports and E_Ports in the fabric. To do this, configure security on the devices that support security: Switch_1, Switch_2, and HBA_1.

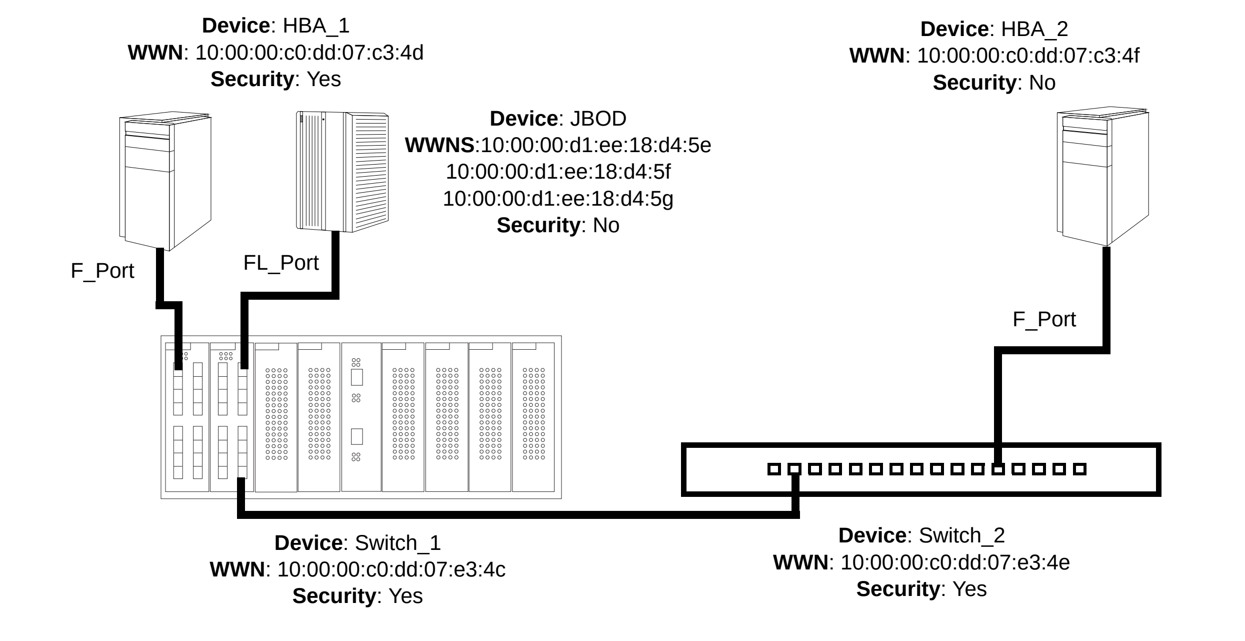


Figure 2-2 Security Example: Switches and HBAs

1. Create a security set (Security_Set_1) on Switch_1.

   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1, HBA_1, and JBOD as members.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210
JBOD	Node WWN: 10:00:00:d1:ee:18:d4:5e Authentication: None
	Node WWN: 10:00:00:d1:ee:18:d4:5f Authentication: None
	Node WWN: 10:00:00:d1:ee:18:d4:5g Authentication: None

- Switch_1 and all devices and switches connected to Switch_1 must be included in the group even if the switch or devices does not support authentication. Otherwise, the Switch_1 port will isolate.
- You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
- For CHAP authentication, create 32-character hexadecimal or 16-character ASCII secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1 and Switch_2 as members. The Switch_1 secret must be shared with the Switch_2 security database.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdef abcdef012 Binding: None

2. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
3. Save and activate Security_Set_1 on Switch_1.
4. Create a security set (Security_Set_2) on Switch_2. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_1 and Switch_2 as members. This is a replication of the entries in ISL group in the Switch_1 security database.

Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Secret: abcdef abcdef012 Binding: None

5. Save and activate Security_Set_2 on Switch_2.

Security Example: RADIUS Server

Consider the fabric shown in Figure 2-3. This fabric is similar to the one shown in Figure 2-2 with the addition of Radius_1 acting as a RADIUS server. Authorization and authentication is passed from the switch to Radius_1 in the following cases:

- HBA_1 login to Switch_1
- Switch_1 login to Switch_2
- Switch_2 login to Switch_1

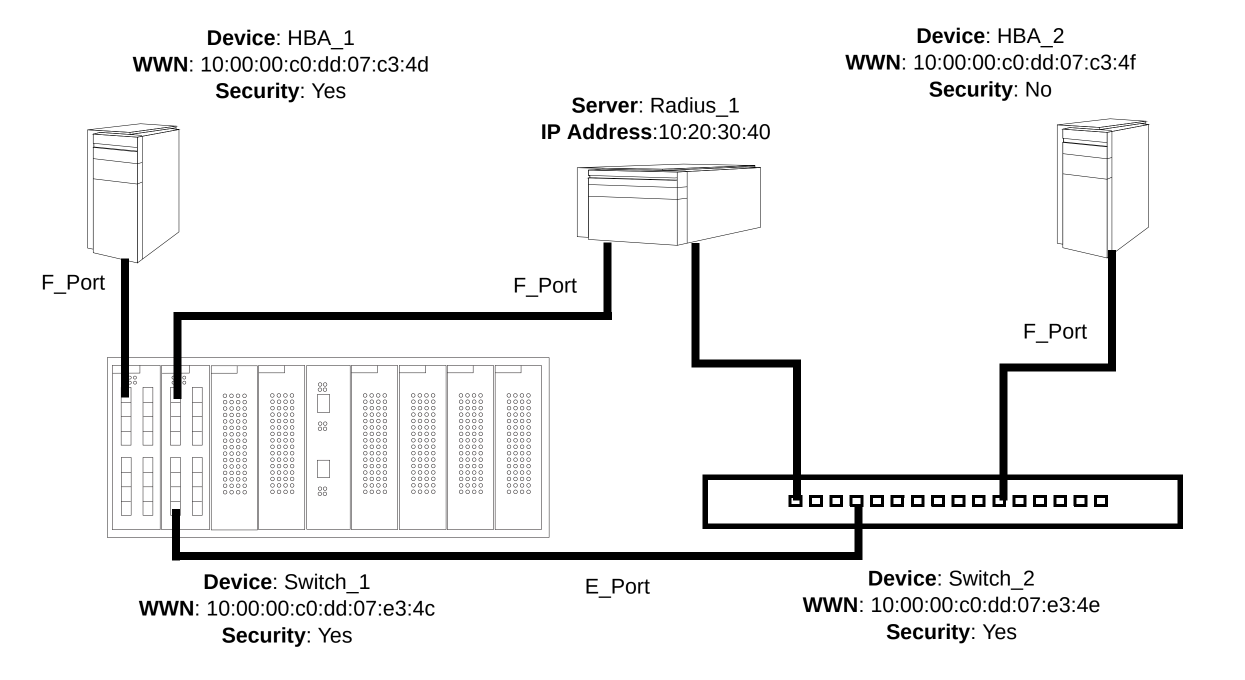


Figure 2-3 Security Example: RADIUS Server

1. Configure the Radius_1 host as a RADIUS server on Switch_1 and Switch_2 to authenticate device logins. Specify the server IP address and the secret with which the switches will authenticate with the server. Configure the switches so that devices authenticate through the switches only if the RADIUS server is unavailable.

Device Authentication Order	RadiusLocal – Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
Total Servers	1 – Enables support for one RADIUS server
Device Authentication Server	True – Enables Radius_1 to authenticate device logins.
Server IP Address	10.20.30.40
Secret	1234567890123456 – 16-character ASCII string (MD5 hash). This is the secret that allows direct communication with the RADIUS server.

2. Create a security set (Security_Set_1) on Switch_1.

   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1 and HBA_1 as members.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210

- Switch_1 and all devices and switches connected to Switch_1 must be included in the group even if the switch or device does not support authentication. Otherwise, the Switch_1 port will isolate.
- You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
- For CHAP authentication, create 32-character hexadecimal or 16-character ASCII secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1 and Switch_2 as members. The Switch_1 secret must be shared with the Switch_2 security database.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef012 Binding: None

3. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged (CHAP) for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
4. Save and activate Security_Set_1 on Switch_1.
5. Create a security set (Security_Set_2) on Switch_2. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_1 and Switch_2 as members.

Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef0123 Binding: None
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None

6. Save and activate Security_Set_2 on Switch_2.

Security Example: Host Authentication

Consider the fabric shown in Figure 2-4. In this fabric, only Switch_2 and HBA_2/APP_2 support security, where APP_2 is a host application. The objective is to secure the management server on Switch_2 from unauthorized access by an HBA or an associated host application.

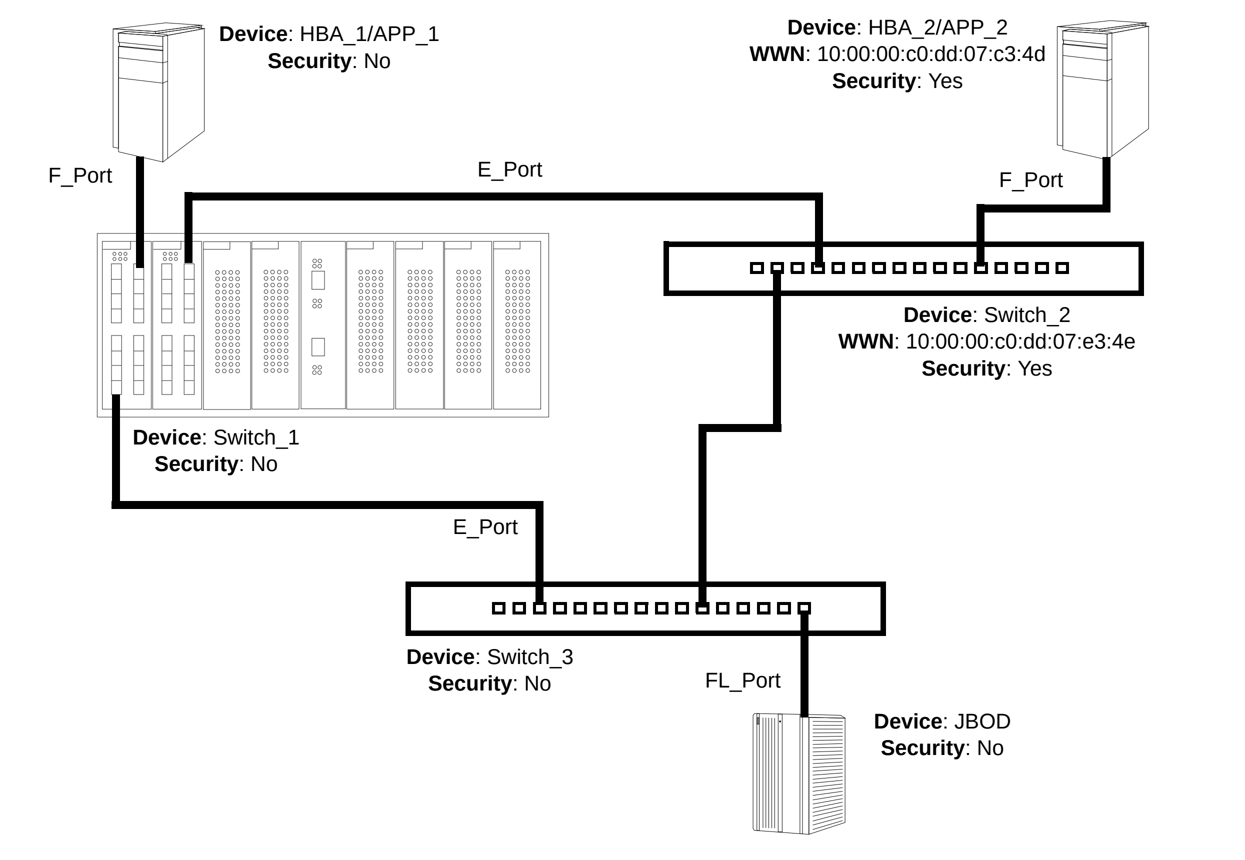


Figure 2-4 Security Example: Management Server

1. Create a security set (Security_Set_2) on Switch_2.
2. Create a Management Server group (Group_1) in Security_Set_2 with Switch_2 and HBA_2 or APP_2 as its member.

   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For MD5 authentication, create secrets.

Switch_2	Node WWN: 10:00:00:c0:dd:07:c3:4e CT Authentication: True Hash: MD5 Secret: 9876543210fedcba9
HBA_2 or APP_2	Node WWN: 10:00:00:c0:dd:07:c3:4d CT Authentication: True Hash: MD5 Secret: fedcba9876543210

3. Configure security on HBA_2 or APP_2 using the appropriate management tool. Logins between the Switch_2 and HBA_2 or APP_2 will be challenged (MD5) for their respective secrets. Therefore, the secrets that you configured for HBA_2 or APP_2 on Switch_2 must also be configured on HBA_2 or APP_2.
4. Save and activate Security_Set_2.

Fabric Management

The Enterprise Fabric Suite 2007 application executes on a management workstation that provides for the configuration, control, and maintenance of multiple fabrics. Supported platforms include Windows, Solaris, Linux, and MacOS X.

The browser-based application, QuickTools, and the command line interface (CLI) reside in the switch firmware and provide for the management of individual switches in a single fabric. Consider how many fabrics will be managed, how many management workstations are needed, and whether the fabrics will be managed with Enterprise Fabric Suite 2007, QuickTools, or the CLI.

A switch supports a combined maximum of 19 logins 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 Enterprise Fabric Suite 2007 logins, QuickTools logins, API logins, and Telnet logins

Additional logins will be refused.

3 Installation

This section describes how to install and configure the QLogic 9000 Series switch. The following topics are covered:

- Site Requirements
- Installing a Switch
- Installing Firmware
- Adding a Switch to an Existing Fabric
- Installing Feature License Keys
- HyperStacking

Site Requirements

Consider the following items when installing a QLogic 9000 Series switch:

- Fabric Management Workstation
- Switch Power Requirements
- Environmental Conditions

28

Fabric Management Workstation

The requirements for fabric management workstations running Enterprise Fabric Suite 2007 are described in Table 3-1:

Table 3-1. Management Workstation Requirements

Operating System	■ Windows® 2003 and XP SP1/SP2 ■ Solaris™ 9,10, and 10 x86 ■ Red Hat® Enterprise Linux® 4, 5 ■ SUSE™ Linux Enterprise Server 9, 10 ■ Mac® OS X 10.4, 10.5
Memory	512 MB minimum; 1GB or more is recommended
Disk Space	150 MB per installation of Enterprise Fabric Suite 2007
Processor	1 GHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet Browser	■ Microsoft® Internet Explorer® 6.0 and later ■ Netscape® Navigator® 6.0 and later ■ FireFox® 1.5 and later ■ Safari® 1.0 and later (Windows and Mac OS) ■ Java 2 Standard Edition Runtime Environment 1.4.2 and later to support the QuickTools web applet

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

Switch Power Requirements

Power requirements are 10 Amps at 100 VAC or 4.2 Amps 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 (32–104°F)
- Relative humidity: 15–80%, non-condensing

Installing a Switch

Unpack the switch and accessories. The QLogic 9000 Series switch is shipped with the components shown in Figure 3-1:

- QLogic 9000 Series switch (1) with firmware installed
- Power cords (2)
- Power cord restraint bails (2)
- Rail kit
- RJ-45/RS-232 console adapter (1)
- Software box containing a CD-ROM. The CD-ROM contains the Enterprise Fabric Suite 2007 switch management application, release notes, and documentation.

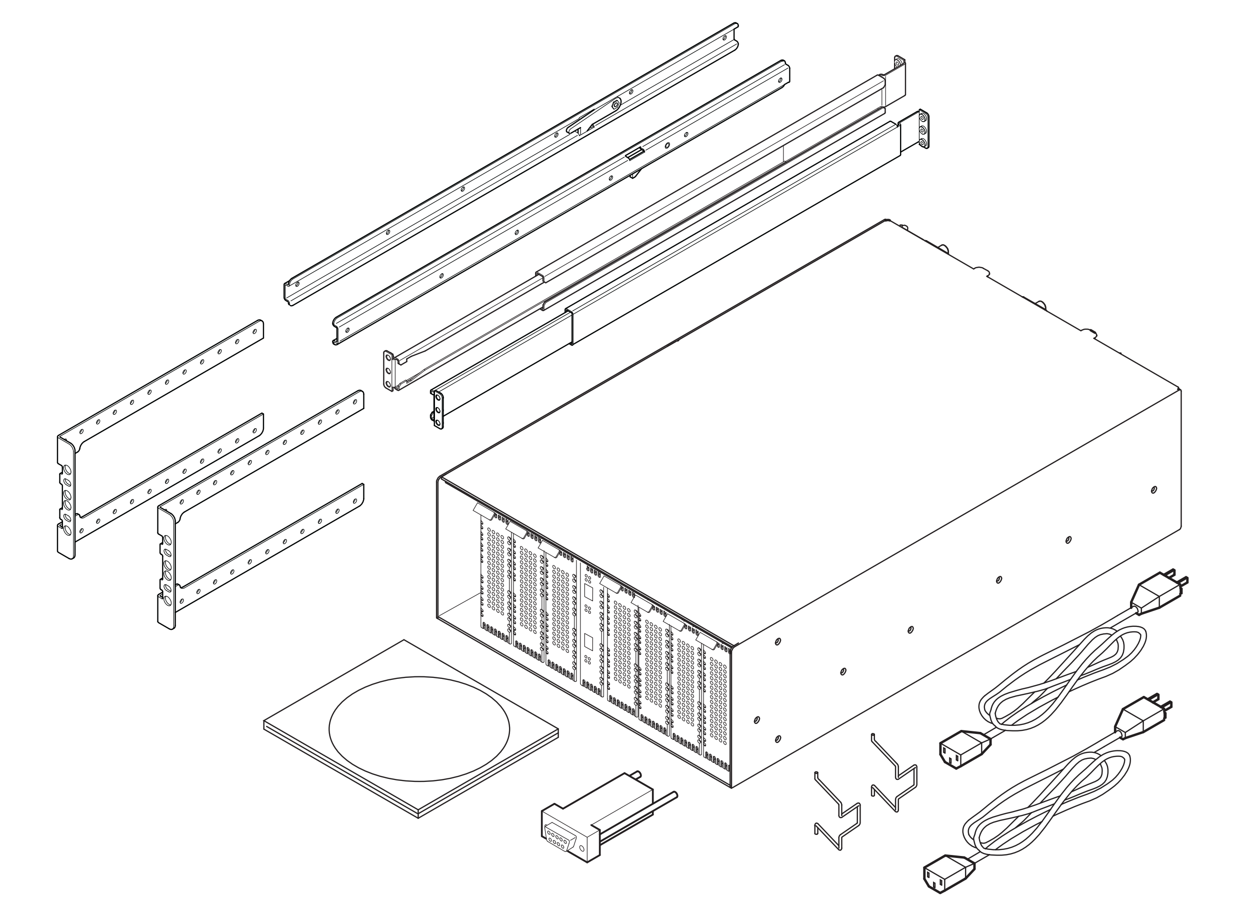


Figure 3-1 QLogic 9000 Series Stackable Chassis Switch

Installing a QLogic 9000 Series switch involves the following steps:

1. Mount the Switch
2. Stack the Switches
3. Install I/O Blades
4. Install Transceivers
5. Power Up the Switch
6. Configure the Workstation
7. Connect the Workstation to the Switch
8. Install Enterprise Fabric Suite 2007
9. Start Enterprise Fabric Suite 2007
10. Configure the Switch
11. Cable Devices to the Switch

Mount the Switch

WARNING!!

Mount switches in the rack so that the weight is distributed evenly. An unevenly loaded rack can become unstable possibly resulting in equipment damage or personal injury.

AVERTISSEMENT!!

Installer les commutateurs dans l’armoire informatique de sorte que le poids soit réparti uniformément. Une armoire informatique déséquilibré risque d'entraîner des blessures ou d'endommager l'équipement.

WARNUNG!!Switches so in das Rack einbauen, dass das Gewicht gleichmäßig verteilt ist. Ein Rack mit ungleichmäßiger Gewichtsverteilung kann schwanken/umfallen und Gerätbeschädigung oder Verletzung verursachen.

¡ADVERTENCIA!Monte los conmutadores en el estante de modo que el peso se distribuya de manera uniforme. Un estante cuya carga no esté distribuida de manera uniforme puede ser inestable y podría dañar el equipo o causar lesiones personales.

CAUTION!

- If the switch is mounted in a closed or multi-unit rack assembly, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature. Refer to “Environmental Factors” on page A-14.
- The switch must rest on rails or a shelf in the rack or cabinet.
- Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the rack for service access and ventilation.
- Multiple rack-mounted units connected to the AC supply circuit may overload that circuit or overload the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit. Refer to “Electrical Requirements” on page A-12.
- Reliable grounding in the rack must be maintained from the switch chassis to the AC power source.

ATTENTION!

- Si le commutateur est monté dans un assemblage fermé ou dans un bâti à plusieurs unités, vérifiez que la température de fonctionnement à l'intérieur de l'armoire du bâti ne dépasse pas la température ambiante maximale assignée. Reportez-vous à la section "Environmental Factors" on page A-14 (Environnement).
- Le commutateur doit reposer sur des rails ou sur une étagère du bâti ou du cabinet.
- N'empêchez pas l'air de circuler dans le châssis. Laissez un espace d'au moins 16 cm (6,5 pouces) à l'avant et à l'arrière du bâti pour l'accès du personnel d'entretien et l'aération.
- Les unités multiples en bâti connectées au circuit d'alimentation en CA peuvent surcharger ce circuit ou le câblage d'alimentation en CA. Vérifiez la capacité de votre source d'alimentation électrique et calculez la puissance totale utilisée par tous les commutateurs du circuit. Reportez-vous à la section "Electrical Requirements" on page A-12 (Exigences en électricité).
- Une mise à la masse fiable doit être maintenue dans le bâti depuis le châssis du commutateur jusqu'à la source d'alimentation en CA.

VORSICHT!

- Wenn der Switch in ein geschlossenes Gestell oder eine Gestelleinheit mit mehreren Geräten eingebaut wird, stellen Sie sicher, dass die Betriebstemperatur im Gestell nicht die maximal zulässige Umgebungstemperatur übersteigt. Lesen Sie dazu "Environmental Factors" on page A-14 (Umgebungsfaktoren).
- Der Switch muss auf Schienen oder auf einem Regal- im Server-Rack oder -Schrank liegen.
- Schränken Sie den Luftstrom im Gehäuse nicht ein. Lassen Sie einen Mindestabstand von 16 cm am vorderen und hinteren Rand des Regals für Wartungsarbeiten und Ventilation.
- Der Anschluss von mehreren in ein Gestell eingebauten Einheiten an den Netzstromkreis kann zu einer Überlastung dieses Stromkreises oder der Netzverkabelung führen. Berücksichtigen Sie die Kapazität der Stromquelle und die Gesamt-Leistungsaufnahme aller an diesen Stromkreis angeschlossenen Switches. Lesen Sie dazu "Electrical Requirements" on page A-12 (Elektrische Voraussetzungen).
- Zuverlässiges Erden im Regal muss vom Switch-Gehäuse zur Netzstromquelle gepflegt werden.

¡PRECAUCIÓN!

- Si el conmutador se monta en un ensamblaje de estante cerrado o de varias unidades, asegúrese de que la temperatura de funcionamiento dentro del alojamiento del estante no supere la temperatura ambiental máxima permitida. Consulte el apartado relativo a los "Environmental Factors" on page A-14 (factores medioambientales).
- El conmutador debe descansar sobre rieles o sobre una tabla del estante o alojamiento.
- No restrinja el flujo de aire del chasis. Deje como mínimo 16 cm (6,5 pulgadas) de separación en la parte delantera y trasera del estante de modo que tenga ventilación y se pueda acceder a él en caso de reparación.
- Es posible que si se conectan varias unidades montadas en estante al circuito de alimentación de CA, dicho circuito o el cableado de alimentación de CA se sobrecarguen. Tenga en cuenta la capacidad de la fuente de alimentación y el consumo total de alimentación de todos los conmutadores del circuito. Consulte el apartado relativo a los "Electrical Requirements" on page A-12 (requisitos eléctricos).
- Se debe mantener una conexión fiable en el estante desde el chasis del conmutador a la fuente de alimentación de CA.

The switch is designed to be mounted in a rack using the mounting brackets and the QLogic 9000 Series rail kit shown in Figure 3-2. To mount the switch in a rack, do the following. Rack mounting instructions can also be found in the *QLogic 9000 Series Stackable Chassis Switch Rack Mounting Guide* packaged with the switch.

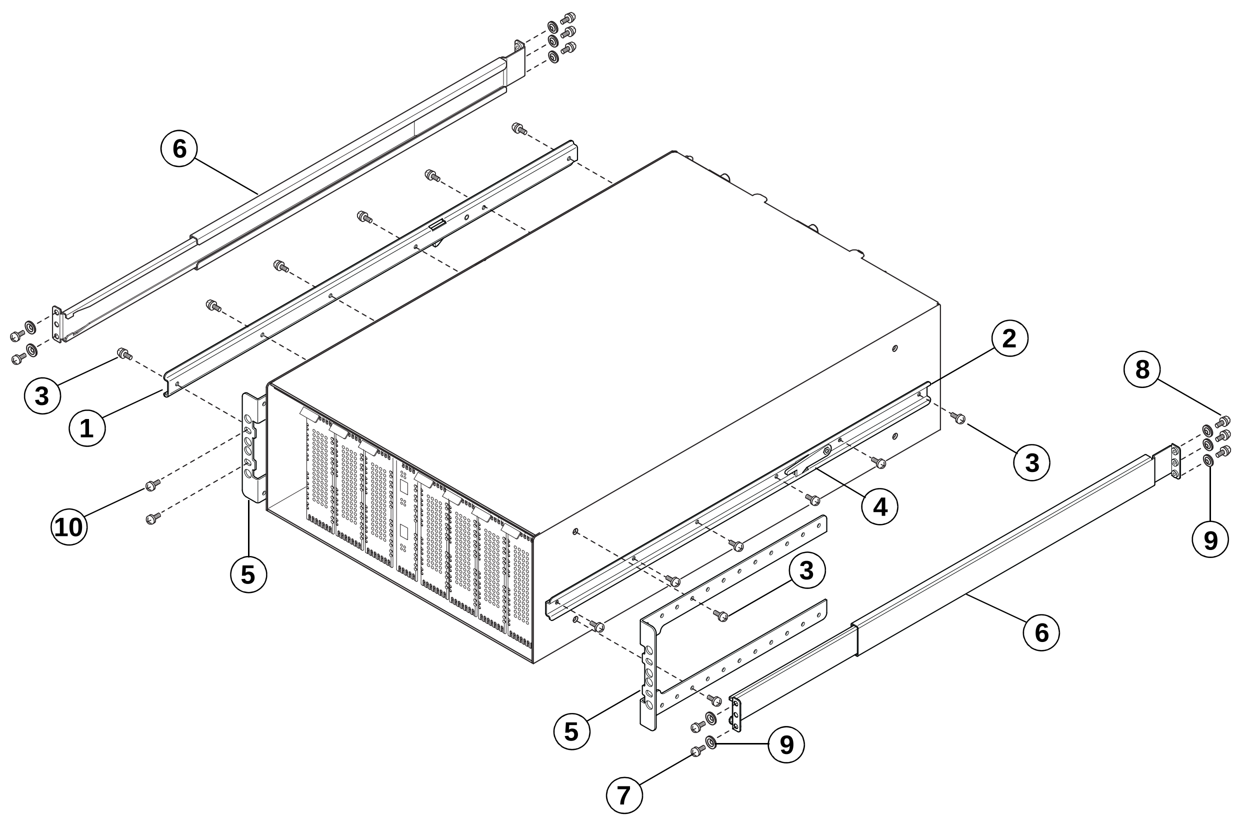


Figure 3-2 QLogic 9000 Series Rail Kit

1. Install left (1) and right (2) switch rails on the switch using six 8-32 screws (3) for each. Be sure that the latch is closest to the end of the switch that will be installed first in the rack and that the latch tab (4) is pointing down.

   WARNING!!

   If the switch rails are not installed properly, the switch could slide out of the rack rails causing damage to the switch and serious personal injury.

   AVERTISSEMENT!!

   Lorsque les rails du commutateur ne sont pas installés correctement, le commutateur peut glisser hors des rails du bâti, ce qui peut endommager le commutateur et entraîner de graves blessures.

   WARNUNG!!

   Wenn die Switch-Schienen nicht richtig installiert wurden, könnte der Switch aus den Regalschienen rutschen und dadurch könnte er beschädigt und Personen schwer verletzt werden.

   ¡ADVERTENCIA!

   Si los rieles del conmutador no están instalados correctamente, el conmutador podría deslizarse y salirse de los rieles del estante y estropear el conmutador además de causar graves lesiones personales.

2. Install the brackets (5) on the front or rear corners of the switch with two 8-32 screws to produce the desired setback. Allow minimum clearances for cabling of 2 inches for the I/O blade side and 8 inches for the Fan blade side.

   - For a fans-first installation, install the brackets on the front corners of the switch.
   - For a faceplate-first installation, install the brackets on the rear corners of the switch.

   These instructions assume a fans-first installation.

3. Extend the rack rails (6) to fit the inner dimensions of the rack. The rail flanges on both ends fit inside the rack. Be sure that the inner rail is toward the front. Fasten the front rail flange to the rack with two 10-32 screws (7) using the upper and lower holes. Fasten the rear end of the rail to the rack with three 10-32 screws (8). For racks with square holes, use a centering washer (9) with each screw.

4. Slide the switch and rail assembly into the rack rails. Fasten the switch to the rack with two screws (10), one through each bracket.

Install I/O Blades

I/O blades are ordered and shipped separately so that you can customize your switch for the performance you need. The following I/O blades are available:

- FC8G16–Fibre Channel 8/4/2/1-Gbps I/O blade
- FC4G16–Fibre Channel 4/2/1-Gbps I/O blade
- FC10G4–Fibre Channel 10-Gbps I/O blade.

Any I/O blade can be installed in any I/O slot. To install I/O blades, do the following:

1. Remove I/O panels as needed to match the number of I/O blades to be installed. Pull the I/O panel by the latch to disengage and remove. Every I/O slot must have an I/O blade or an I/O panel to ensure proper cooling.
2. Install I/O blades. Open the I/O blade latch and slide the I/O blade into the chassis until it makes contact with the midplane connector. Rotate the latch upward to lock the I/O blade in place.

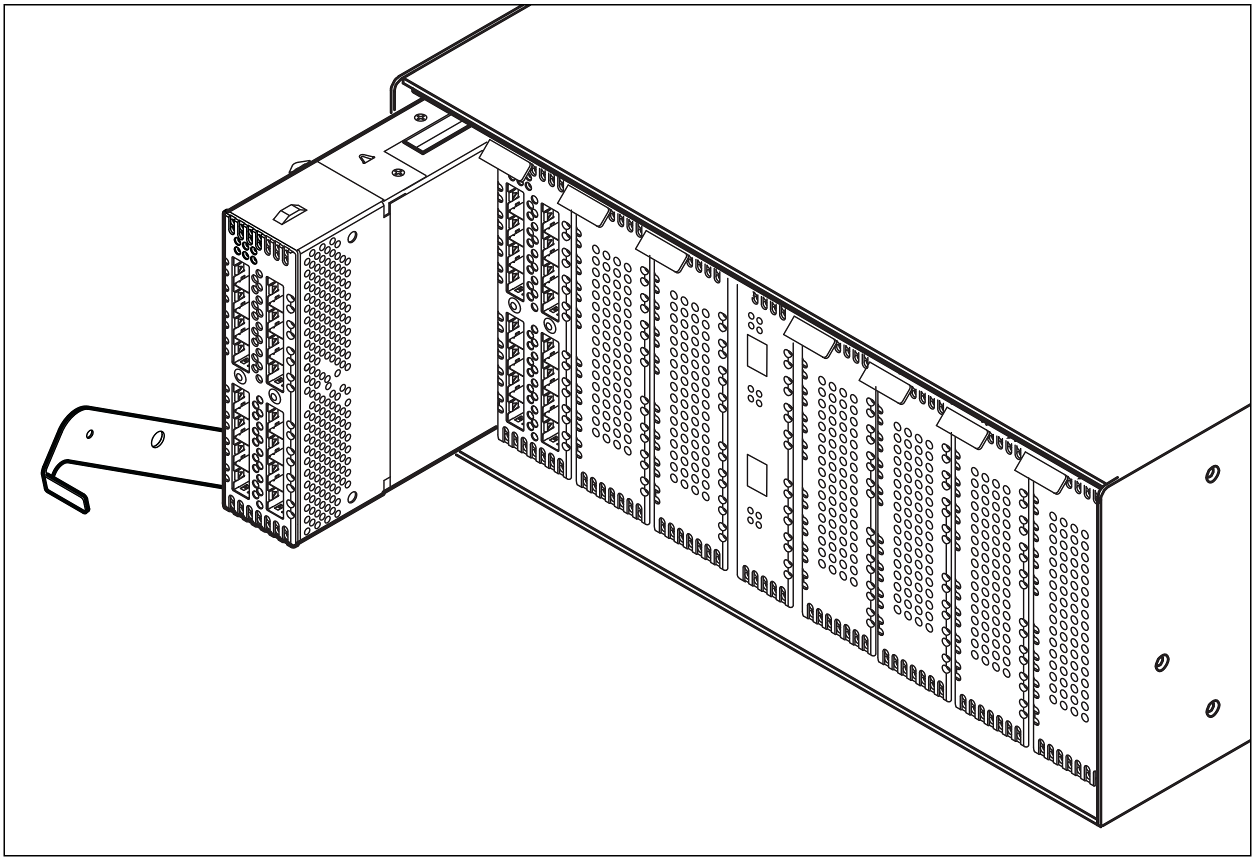


Figure 3-3 Installing an I/O Blade

Stack the Switches

10-Gbps stacking cables are available to connect two QLogic 9000 Series switches or a QLogic 9000 Series switch and a QLogic 5000 Series switch as shown in Figure 3-4.

- To connect two QLogic 9000 Series switches, use an X2-X2 cable. Install the cable connectors in the respective switch ports with the circuit boards on the left. The cable connector will fit only one way as shown in Figure 3-4.
- To connect a SANbox 5000 Series switch and a QLogic 9000 Series switch, use an XPAK-X2 cable. Install the XPAK connector in the SANbox 5000 series switch port with the circuit board toward the mid line of the switch. Install the X2 connector in the QLogic 9000 Series switch port with the circuit board on the left.

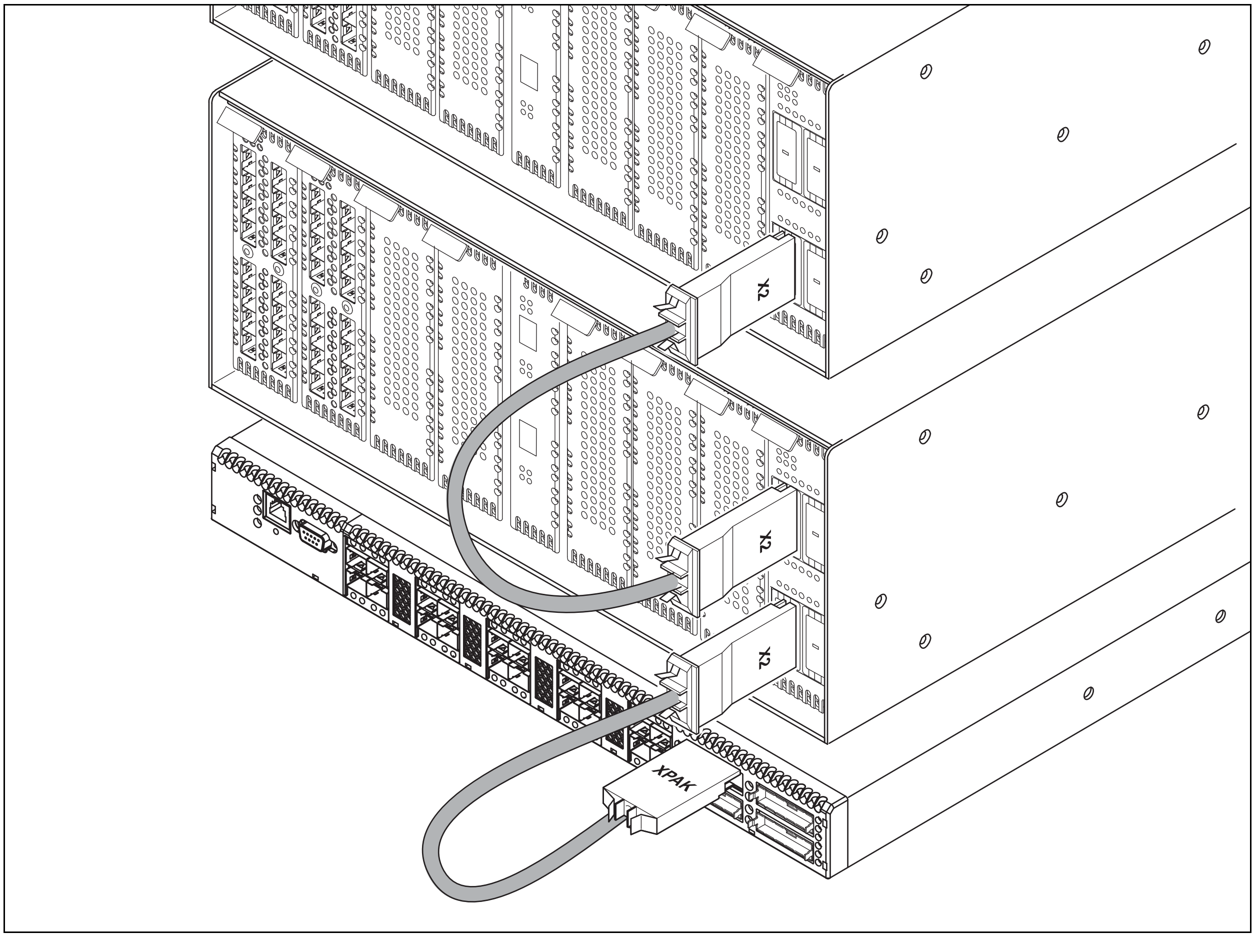


Figure 3-4 Installing Stacking Cables

Install Transceivers

The switch supports a variety of SFP and X2 transceivers. To install a transceiver, insert the transceiver into the port and gently press until it snaps in place. To remove a transceiver, pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

NOTE:

The transceiver will fit only one way. If the transceiver does not install under gentle pressure, flip it over and try again.

10-Gbps I/O blades come with port covers in the ports. Before installing the stacking cables or transceivers remove the port covers. To remove a port cover, insert a small flathead screwdriver in the cover slot and gently pry the cover from the port.

CAUTION!

To maintain proper air flow and prevent the switch from overheating, keep covers installed in unused 10-Gbps ports.

ATTENTION!

Pour assurer un bon flux d'air et éviter une surchauffe du commutateur, laissez les caches sur les ports 10 Gb/s non utilisés.

VORSICHT!

Um eine Luftströmung aufrecht zu erhalten und eine Überhitzung des Switches zu vermeiden, lassen Sie die Abdeckung an nicht verwendeten 10GBit/s-Ports installiert.

¡PRECAUCIÓN!

Para mantener un flujo de aire adecuado y evitar que el conmutador se caliente excesivamente, mantenga las cubiertas instaladas en puertos de 10 Gbps sin utilizar.

Power Up 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 chassis. 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 13 Amps and be approved by UL and CSA.
- For 250 Volt electrical service: The cable must be rated at 13 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

AVERTISSEMENT!!

Pour la sécurité de l'utilisateur, l'appareil est livré avec un câble d'alimentation trifilaire et une fiche. Pour éviter toute secousse électrique, enficher ce câble à une prise correctement mise à la terre.Une prise électrique dont les fils sont mal branchés peut créer une tension dangereuse dans les pièces métalliques du châssis switch. Pour éviter toute secousse électrique, s'assurer que les fils sont correctement branchés et que la prise est bien mise à la terre.

Dans certains pays les prises électriques sont de modèle différent; on ne peut y enficher le câble de l'appareil. On doit donc en utiliser un autre ayant les caractéristiques suivantes:

- Alimentation 125 V: Câble pour courant nominal de 13 A, agréé LAC et CSA.
- Alimentation 250 V: Câble pour courant nominal de 13 A, conforme au H05VV-F, et agréé VDE, SEMKO et DEMKO.

WARNUNG!!

Dieses Produkt wird mit einem 3-adrigen Netzkabel mit Stecker geliefert. Dieses Kabel erfüllt die Sicherheitsanforderungen und sollte an einer vorschriftsmäßigen Schukosteckdose angeschlossen werden, um die Gefahr eines elektrischen Schlages zu vermeiden.Elektrosteckdosen, die nicht richtig verdrahtet sind, können gefährliche Hochspannung an den Metallteilen des switch-Gehäuses verursachen. Der Kunde trägt die Verantwortung für eine vorschriftsmäßige Verdrahtung und Erdung der Steckdose zur Vermeidung eines elektrischen Schlages.

In manchen Ländern ist eventuell die Verwendung eines anderen Kabels erforderlich, da der Stecker des mitgelieferten Kabels nicht in die landesüblichen Steckdosen paßt. In diesem Fall müssen Sie sich ein Kabel besorgen, daß die folgenden Anforderungen erfüllt:

- Für 125 Volt-Netze: 13 Ampere Kabel mit UL- und CSA-Zulassung.
- Für 250 Volt-Netze: 13 Ampere Kabel gemäß den Anforderungen der H05VV-F und VDE-, SEMKO- und DEMKO-Zulassung.

¡ADVERTENCIA!

Para garantizar la seguridad del usuario, este producto se suministra con un cable de alimentación de 3 hilos y un enchufe. Utilice este cable de alimentación junto con un enchufe correctamente conectado a tierra para evitar descargas eléctricas. Un enchufe eléctrico que no esté correctamente conectado puede hacer que las piezas metálicas del chasis del conmutador tengan un voltaje peligroso. Es responsabilidad del cliente asegurarse de que el enchufe esté correctamente conectado a una toma de tierra para evitar descargas eléctricas.

Es posible que en algunos países necesite un cable de alimentación diferente porque el enchufe del cable suministrado con el equipo no se ajusta a su enchufe eléctrico. En este caso, debe proveerse de su propio cable de alimentación. El cable que utilice debe cumplir los siguientes requisitos:

- Para un servicio eléctrico de 125 voltios, el cable debe tener una corriente nominal de 13 amperios y estar aprobado por UL y CSA.
- Para un servicio eléctrico de 250 voltios, el cable debe tener una corriente nominal de 13 amperios, cumplir los requisitos de H05VV-F y estar aprobado por VDE, SEMKO y DEMKO.

The switch comes with two NEMA 5-15, non-locking, power cords (SKU: CPK-9000-US). This power cord is approved for North America (USA, Canada, Puerto Rico), Mexico, Central America, South America, Korea, Taiwan, Phillippines, and Thailand. Refer to Table A-10 for information about power cords for other regions/countries.

To power up the switch, do the following:

1. Attach a power cord restraint bail to each Power Supply blade as show in Figure 3-5.
2. Connect the power cords firmly to the Power Supply blade AC power receptacles.
3. Fasten the restraint bail on each plug.
4. Connect each power cord to a 3-wire, grounded, AC outlet that delivers power in accordance with the power requirements in Appendix A.

   NOTE:

   To provide redundancy in the event of an AC power circuit failure, connect the Power Supply blades to separate AC circuits.

5. Place the On/Off switches on both Power Supply blades in the On position. The power-up sequence will take a few minutes. The switch is operational when both CPU Heartbeat LEDs are flashing once per second.

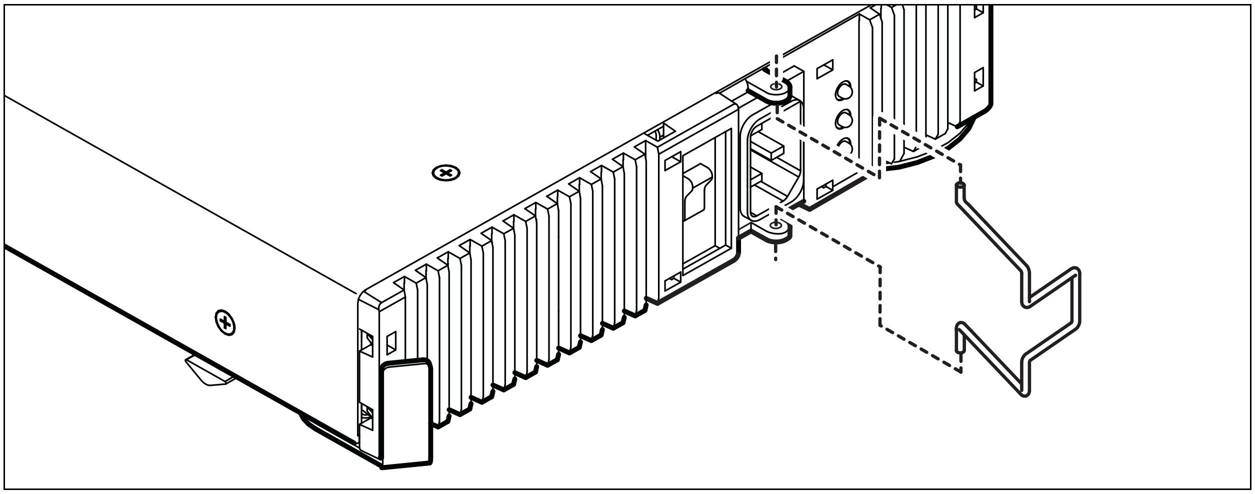


Figure 3-5 Attaching the Power Cord Restraint Bail

Configure the Workstation

If you plan to use the command line interface 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. If you plan to use Enterprise Fabric Suite 2007 or QuickTools to manage the switch, the Configuration Wizard manages the workstation IP address for you – proceed to "Install Enterprise Fabric Suite 2007" on page 3-18.

NOTE:

If you are using Enterprise Fabric Suite 2007 to manage the switch on a Windows workstation, be sure that you have an active Ethernet connection when you boot the workstation.

Setting the Workstation IP Address for Ethernet Connections

The default IP address of the CPU0 Ethernet port is 10.0.0.1. To ensure that your workstation is configured to communicate with the 10.0.0 subnet, refer to the following instructions for your workstation.

- For a Windows workstation, do the following:

  1. Click the **Start** button, then choose **Settings**>**Control Panel**>**Network and Dial-Up Connections**.
  2. Choose **Make New Connection**.
  3. Click the **Connect to a private network through the Internet** radio button then click the **Next** button.
  4. Enter 10.0.0.253 for the IP address.

- For a Linux or Solaris 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
```

- For a MacOS X workstation, do the following:

  1. Choose **System Preferences>System Preferences>Network**.
  2. Double-click your network adapter.
  3. In the configuration dialog, select **Manually** from the Configure IPv4 drop down menu.
  4. Enter 10.0.0.253 in the IP Address field.
  5. Enter 255.255.255.0 in the Subnet Mask field.
  6. Click **Apply Now**.

Configuring the Workstation Serial Port

To configure the workstation serial port, do the following:

1. Connect the RS-232/RJ-45 console adapter to a COM port on the management workstation.
2. Connect an Ethernet 10/100 Base-T straight cable to the console adapter and to the RJ-45 serial port on the switch.
3. Configure the workstation serial port according to your platform:

   - For Windows:

     a. Open the HyperTerminal application. Choose the **Start** button, select **All Programs>Accessories>Communications> HyperTerminal**.

     b. Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the **OK** button.

     c. Enter the following COM Port settings in the COM Properties window and choose the **OK** button.

        ❑ Bits per second: 9600

        ❑ Data Bits: 8

        ❑ Parity: None

        ❑ Stop Bits: 1

        ❑ Flow Control: None

   - For Linux:

     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
        ```

        `pr portdev/ttyS0` specifies port 0 on the workstation. Choose "pr" setting to match the workstation port to which you connected the switch.

     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.

- For Solaris: Modify the /etc/remote file and locate the `hardwire` entry. Choose the `:dv=/dev/term/` setting to match the workstation port (a or b) to which you connected to the switch.

```
hardwire:\:dv=/dev/term/a:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:
```

4. Proceed to “Power Up the Switch” on page 3-13.

Connect the Workstation to the Switch

You can manage the switch using Enterprise Fabric Suite 2007, the QuickTools web applet, or the command line interface. Enterprise Fabric Suite 2007 and QuickTools require a connection to the CPU0 Ethernet port. The command line interface can use an Ethernet connection or a serial connection to the primary CPU blade. Choose a switch management method, then connect the management workstation to the switch in one of the following ways:

- Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. You can use a 10/100 Base-T straight or cross-over cable. The default active Ethernet port is located on the CPU0 CPU blade on the back of the switch.
- Serial port connection from the management workstation to the switch RJ-45 serial port connector on the CPU0 blade. This requires the RS-232/RJ-45 console adapter provided with the switch and a 10/100 Base-T straight cable.

Install Enterprise Fabric Suite 2007

You can install Enterprise Fabric Suite 2007 on a Windows, Linux, Solaris, or MacOS X® workstation. To install the Enterprise Fabric Suite 2007 application, refer to the *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide*.

Obtain the Network Configuration

Obtain the IP address and subnet mask from your network administrator. The workstation must have the same subnet as the switch.

Start Enterprise Fabric Suite 2007

NOTE:

After the switch is operational, you can also open the QuickTools web applet, by entering the switch IP address in an internet browser. Refer to the *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide* for more information.

To start Enterprise Fabric Suite 2007, do the following.

1. Start the Enterprise Fabric Suite 2007 using one of the following methods:

   ■ For Windows, double-click the Enterprise Fabric Suite 2007 shortcut, or select **Enterprise Fabric Suite 2007** from Start menu, depending on how you installed the Enterprise Fabric Suite 2007 application. From a command line, you can enter the Enterprise_Fabric_Suite_2007 command:

   ```
   <install_directory>Enterprise_Fabric_Suite_2007.exe
   ```

   ■ For Linux, Solaris, or MacOS X, enter the following command:

   ```
   <install_directory>./Enterprise_Fabric_Suite_2007
   ```

2. In the Initial Start dialog, click the **Open Configuration Wizard** button. The Configuration Wizard recognizes the switch and leads you through the configuration process.

Configure the Switch

You can configure the switch using the Enterprise Fabric Suite 2007 application, the QuickTools web applet, or the command line interface. To configure the switch using Enterprise Fabric Suite 2007, click the **Open Configuration Wizard** radio button in the Initial Start dialog, then click the **Proceed** button. The Configuration wizard prompts you for the network configuration information listed in Table 3-2.

Table 3-2. Network Configuration Parameters

Temporary IP address	
Temporary subnet mask	
Current Admin account password	Factory default is *password.*
Archive template file	
Switch domain ID (1–-239)	
Domain ID Lock (Locked/Unlocked)	
Switch name	
Permanent IP address	
Permanent subnet mask	
Permanent gateway address	
Permanent network discovery method	
Ethernet port selection	
Date and time	
New Admin account password	
Create a configuration archive?	

To configure the switch using the command line interface, do the following:

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

   - Ethernet (all platforms): Open a Telnet session with the default switch IP address and log in to the switch with account name *admin* and the default password *password*.

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

- Serial – Windows: Open the HyperTerminal application on a Windows platform.

    a. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.

    b. Select the connection you created earlier and choose the **OK** button.

- Serial – Linux: Open a command window and enter the following command:

```
minicom
```

- Serial – Solaris: Open a command window and enter the following command:

```
tip hardwire
```

2. Open an admin session and enter the Set Setup System command. Enter the values you want for switch IP address (EthNetworkAddress) and the network mask (EthNetworkMask).

```
QLogic #> admin start
QLogic (admin) #> set setup system
```

3. Open a Config Edit session and use the Set Config command to modify the switch configuration.

Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about using the command line interface.

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. LC-type duplex fiber optic cable connectors are designed for SFP transceivers. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

Connect a QLogic 9000 Series switch to a QLogic 5000 series switch through their 10-Gbps ports using an X2-to-XPAK stacking cable. The stacking cable X2 connector is larger than the XPAK connector and attaches to the QLogic 9000 Series 10-Gbps I/O blade.

GL_Ports self configure as FL_Ports when connected to loop of public 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 workstation as new firmware becomes available. You can use the Enterprise Fabric Suite 2007 application, the QuickTools web applet, or the CLI to install new firmware.

- Using Enterprise Fabric Suite 2007 to Install Firmware
- Using QuickTools to Install Firmware
- Using the CLI to Install Firmware

You can load and activate version 7.8 firmware 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 permits the installation and non-disruptive activation of the new firmware. Refer to the *Firmware Release Notes* for previous compatible firmware versions.
- 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.

Install firmware on one switch at a time in the fabric. If you are installing firmware on one switch, wait 120 seconds after the activation is complete before installing firmware on a second switch.

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, Enterprise Fabric Suite 2007 and QuickTools sessions reconnect automatically. However, Telnet sessions must be restarted manually.

NOTE:

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 Enterprise Fabric Suite 2007 to Install Firmware

To install firmware using Enterprise Fabric Suite 2007, do the following:

1. Select a switch in the topology display and double-click to open the Faceplate display. Open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload window, click the **Select** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the loading process.
4. Click the **Start** button to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
5. Click the **OK** button to continue firmware installation or click the **Cancel** button to cancel the firmware installation. Enterprise Fabric Suite 2007 will attempt a hot reset, if possible, to activate the firmware without disrupting data traffic. During a non-disruptive activation, all Logged-In LEDs are extinguished for several seconds. If a non-disruptive activation is not possible, Enterprise Fabric Suite 2007 gives you the opportunity to reset the switch and perform a disruptive activation.

Using QuickTools to Install Firmware

To install firmware using QuickTools, do the following:

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 the **Browse** button to change the folder (path) to search for firmware image files. Click the **Rescan** button to search the new folder displayed in the Firmware Image Folder field.
3. Click the **Start** button 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 the **OK** button to continue firmware installation.
5. Click the **Close** button 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. Refer to "One-Step Firmware Installation" on page 3-24.
- 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. Refer to "Custom Firmware Installation" on page 3-26.

Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about the CLI commands.

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, unpacks the image file, and performs 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

To install firmware using the CLI when a File Transfer Protocol (FTP) server is present on the management workstation, use the Firmware Install command. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about the CLI commands.

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.

   ```
   QLogic #> admin start
   QLogic #> 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      : 10.0.0.254
   Source Filename : 7.8.00.xx_ThCP
   About to install image.  Do you want to continue? [y/n] y
   ```

4. When prompted to install the new firmware, enter Yes to continue or No to cancel. Entering Yes 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).
   ```

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

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

6. 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 workstation to the switch.

   - If your workstation has an FTP server, you can enter the Image Fetch command:

   ```
   QLogic (admin) #> image fetch account_name ip_address filename
   ```

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

     ```
     QLogic (admin) #> image tftp ip_address filename
     ```

   - If your workstation has neither an FTP nor a TFTP server, open an FTP session and download the firmware image file by entering 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.

   ```
   QLogic (admin) $>image list
   ```

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

   ```
   QLogic (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.

   ```
   QLogic (admin) $>hotreset
   ```

Adding a Switch to an Existing Fabric

If there are no special conditions to be configured for the new switch, simply plug in the switch and 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 (RARP, BOOTP, and DHCP).

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

NOTE:

If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric.

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

Installing Feature License Keys

Refer to "Feature Licensing" on page 2-5 for information about available license keys. To install a license key using QuickTools or Enterprise Fabric Suite 2007, do the following:

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

To upgrade a switch using the command line interface, refer to the Feature command in the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide*.

HyperStacking

HyperStacking connects two Model 9200 switches through the ICC ports on the two pairs of CPU blades. Two HyperStack kits are required to successfully conect two switches. Each HyperStack kit contains one HyperStack license key and two cables. A medium crosshead screwdriver and six tie wraps are required to successfully connect two switches. HyperStacking is not disruptive and can be done with both switches operational or both switches powered off.

NOTE:

QLogic 9100 model switches do not support the HyperStack feature.

To HyperStack two switches, do the following:

1. Mount the switches in a rack, one on top of the other with no more than 1U of space between them. A cable loom can be installed in this space. Horizontal clearance from the CPU blades to the rack opening or door should be 7–8 inches to allow for HyperStack cabling. Refer to the *SANbox 9000 Series Stackable Chassis Switch Rack Mounting Guide* for detailed mounting instructions.
2. Verify that the two switches have different domain IDs. If they do not, change the domain ID of one of the switches using the Set Config Switch CLI command.
3. Enter the Show Version CLI command to verify that the two switches have version 7.8 firmware or later. Install version 6.6 firmware, if necessary. Refer to “Installing Firmware” on page 3-22 for detailed information.
4. Follow the directions on the *License Key Upgrade* document for each switch. Apply the respective license keys to each switch. Refer to “Installing Feature License Keys” on page 3-28 for detailed information.

5. Use a screwdriver to remove the covers from all ICC ports. Connect a HyperStack cable to one of the ICC ports with the label side up as shown in Figure 3-6. Secure the cable connector with the captive screws.

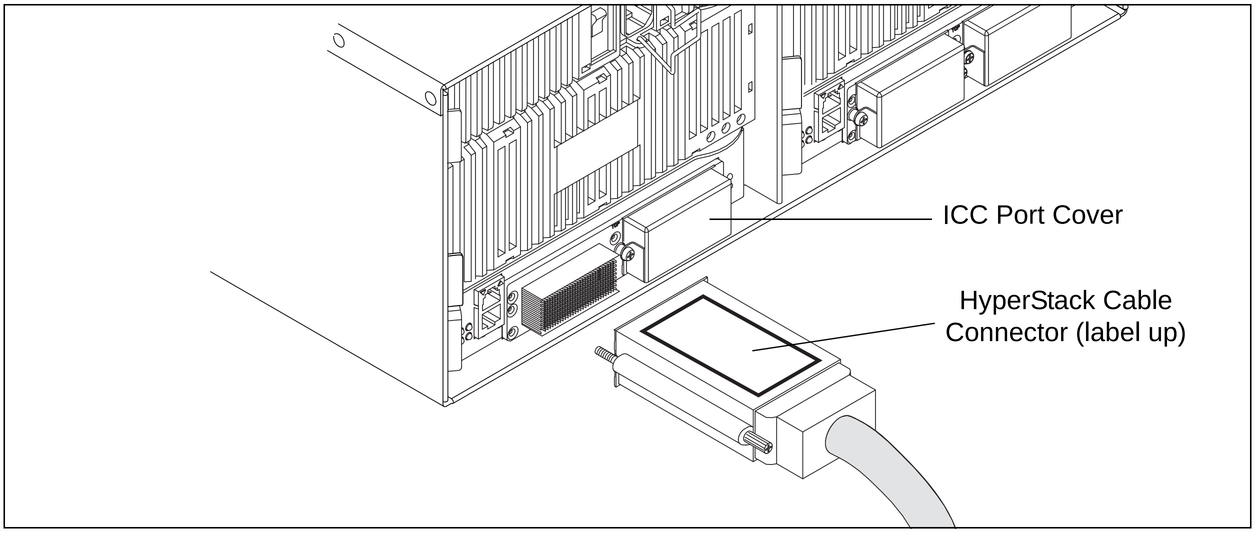


Figure 3-6 HyperStack Cable Connector

6. Connect HyperStack cable connectors as shown in Figure 3-7. These copper cables are very flexible and can be bent as needed without damage. This is the only cabling configuration that is supported. Any other configuration will result in an error.

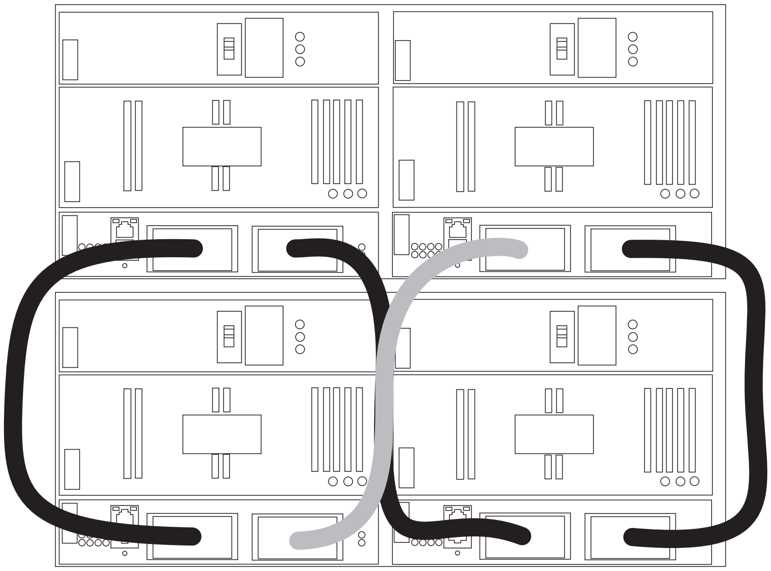


Figure 3-7 Connecting the HyperStack Cables

7. Secure the HyperStack cables in place using ties wraps as shown in Figure 3-8. Secure the outer cables to the rack posts; secure the inner cables to each other. This reduces cable clearance to 7–8 inches and provides room for the removal of the Power Supply and Fan blades on the lower switch.

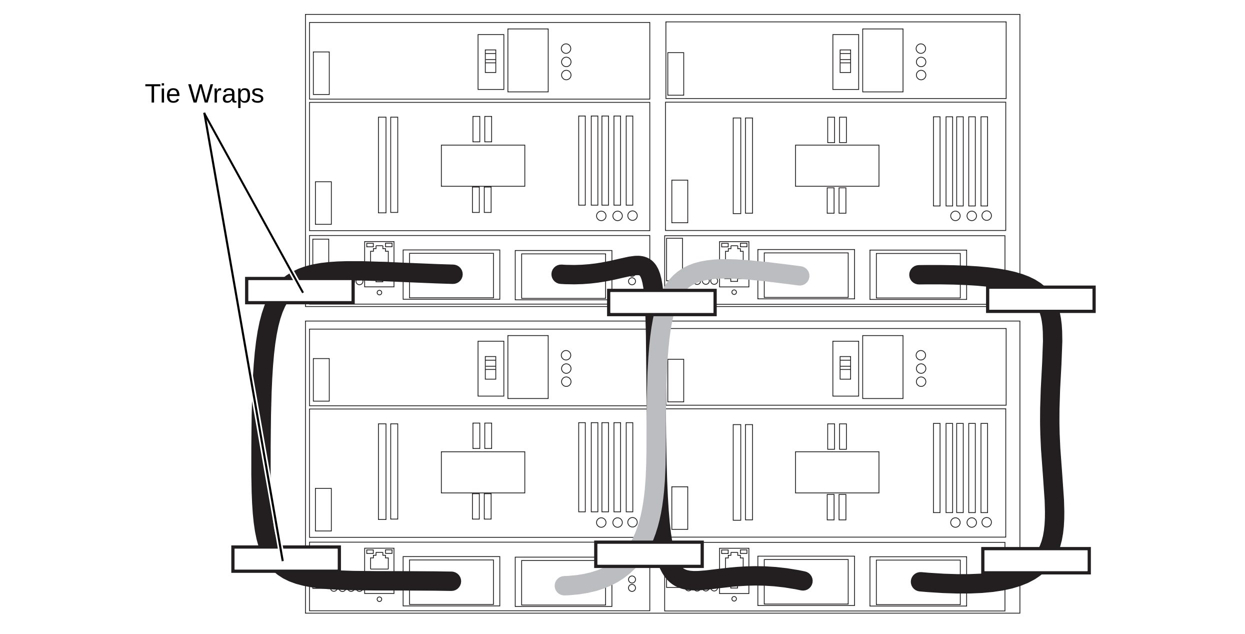


Figure 3-8 Securing HyperStack Cables

8. Confirm that the ICC port Logged-In LEDs are illuminated. This indicates that the switches are communicating.

9. Enter the Show Interconnect CLI command to confirm each ICC port is online.

```
QLogic #> show interconnect

   Blade ID  ICC ID  State         LSDB ID   ISOREASON
   --------  ------  -----         -------   ---------
   CPU0      ICC0    Online        0x1000    NotApplicable
             ICC1    Online        0x1001    NotApplicable

   CPU1      ICC0    Online        0x1010    NotApplicable
             ICC1    Online        0x1011    NotApplicable
```

10. Enter the Show Fabric CLI command to confirm that both QLogic 9000 Series switches are in the fabric.

```
SANbox #> show fabric

 Domain     WWN                      Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                      ------------    ----------      ------------
*1  (0x01)  10:00:00:c0:dd:07:4a:e8  10.20.83.203    0.0.0.0         SANbox 9000
 2  (0x02)  10:00:00:c0:dd:00:6a:2d  10.20.68.12     0.0.0.0         SANbox 9000

  * indicates principal switch
```

Notes

4 Diagnostics/Troubleshooting

This section describes how to recognize, diagnose, and correct problems. Diagnostic information about the switch is available through the various switch LEDs and through the Enterprise Fabric Suite 2007, QuickTools, and CLI event logs and error displays.

The Maintenance Panel presents the Chassis Fault LED as a general index to the switch operational status. The Chassis Fault LED illuminates to indicate faults that have occurred on the CPU blades, I/O blades, Power Supply blades, and Fan blades. The corresponding Fault LED on the blade illuminates to indicate the source of the problem. Following the Fault LEDs to the source and then observing the other LEDs on the blade can provide helpful information. Supporting information from the Enterprise Fabric Suite 2007, QuickTools, or the CLI provide more detailed information.

The following topics describe the Power-on Self Test and the various component diagnostics, concluding with switch recovery.

- Power-On Self Test
- Error Code Blink Patterns
- CPU Blade Diagnostics
- I/O Blade Diagnostics
- FC Port Diagnostics
- Transceiver Diagnostics
- Power Supply Blade Diagnostics
- Fan Blade Diagnostics
- Recovering a Switch Using Maintenance Mode

Power-On Self Test

The switch performs a Power-On Self Test (POST) as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in PROM and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the ASIC

During the POST, the switch logs any errors encountered. If there are no errors, the CPU Heartbeat LED blinks at a steady rate of once per second. If a fatal error occurs, the Chassis Fault LED illuminates and the CPU Heartbeat LED may show an error code blink pattern.

Error Code Blink Patterns

The CPU Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the CPU Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. Refer to "Recovering a Switch Using Maintenance Mode" on page 4-15 for more information about maintenance mode. All other blink patterns indicate critical errors.

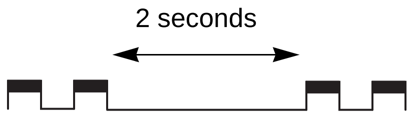
The CPU Heartbeat LED shows an error blink pattern for the following conditions:

- 2 blinks - Internal Firmware Failure Blink Pattern
- 3 blinks - Fatal POST Error Blink Pattern
- 4 blinks - Configuration File System Error Blink Pattern

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. Table 4-1 describes the blink pattern and the actions for this error.

Table 4-1. Internal Firmware Failure Blink Pattern

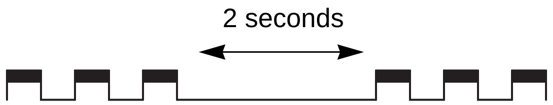


Blade LED	Action
I/O Blade Error LED	Reset the I/O blade.
CPU1 Heartbeat LED	Reset the CPU1 blade
CPU0 Heartbeat LED	The switch is inoperable. Reset the CPU0 blade.

Fatal POST Error Blink Pattern

A fatal POST error blink pattern is 3 blinks followed by a two second pause. The 3-blink error pattern indicates that a POST failure or a system error has occurred. If a system error occurs, contact your authorized maintenance provider. Table 4-2 describes the blink pattern and the actions for this error.

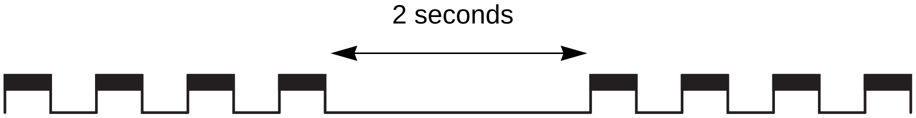
Table 4-2. System Error Blink Pattern



Blade LED	Action
I/O Blade Error LED	Reset the I/O blade.
CPU1 Heartbeat LED	Reset the CPU1 blade.
CPU0 Heartbeat LED	The switch is inoperable. Reset the CPU0 blade.

Configuration File System Error Blink Pattern

A configuration file system error blink pattern is 4 blinks followed by a two second pause and appears only on the CPU Heartbeat LED. 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, do the following:

1. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

   ```
   telnet 10.0.0.1
   ```
   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, password).

3. Open an admin session to acquire the necessary authority.

   ```
   SANbox $>admin start
   ```
4. Restore the configuration. When the restore is complete, the switch will reset.

   ```
   SANbox (admin) $>config restore
   ```
   If a configuration does not exist, enter the Config Backup command, then enter the Config Restore command.

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

      ```
      telnet 10.0.0.1
      ```
      or

      ```
      telnet switchname
      ```
      where *switchname* is the switch name associated with the IP address.

   b. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).

c. Open an admin session to acquire the necessary authority.

```
QLogic $>admin start
```

d. Restore the configuration file. When the restore is complete, the switch will reset.

```
QLogic (admin) $>config restore
```

CPU Blade Diagnostics

Figure 4-1 illustrates the CPU blade diagnostic process. If the corrective action is not successful, contact you authorized maintenance provider.

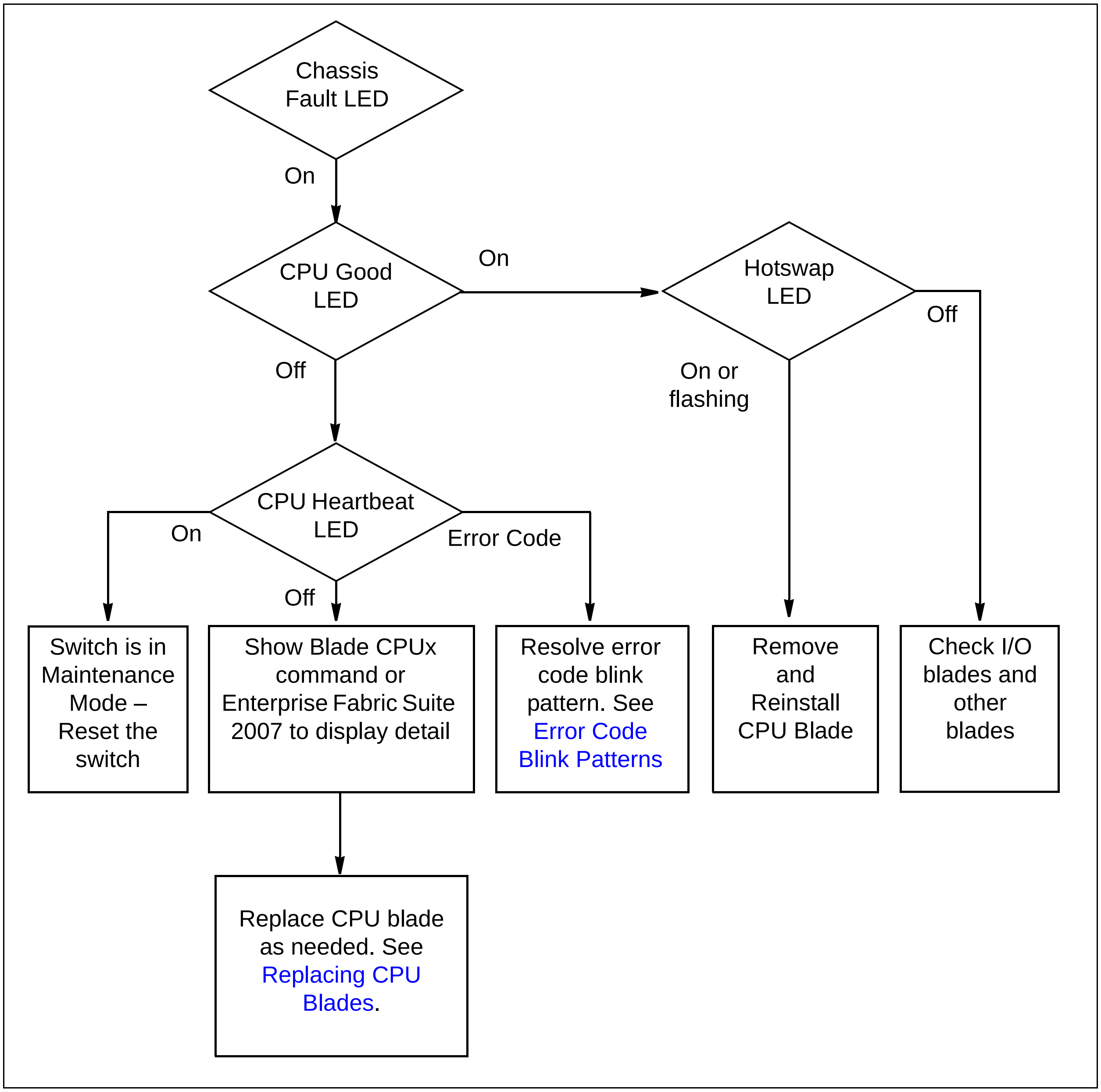

Chassis Fault LED
On
CPU Good LED
On
Hotswap LED
Off
Off
On or flashing
CPU Heartbeat LED
On
Error Code
Off
Switch is in Maintenance Mode – Reset the switch
Show Blade CPUx command or Enterprise Fabric Suite 2007 to display detail
Resolve error code blink pattern. See Error Code Blink Patterns
Remove and Reinstall CPU Blade
Check I/O blades and other blades
Replace CPU blade as needed. See Replacing CPU Blades.

Figure 4-1 CPU Blade Diagnostic Process

I/O Blade Diagnostics

Figure 4-2 illustrates the I/O blade diagnostic process. For port errors indicated by the Logged-In LED, refer to "FC Port Diagnostics" on page 4-8. If the corrective action is not successful, contact you authorized maintenance provider.

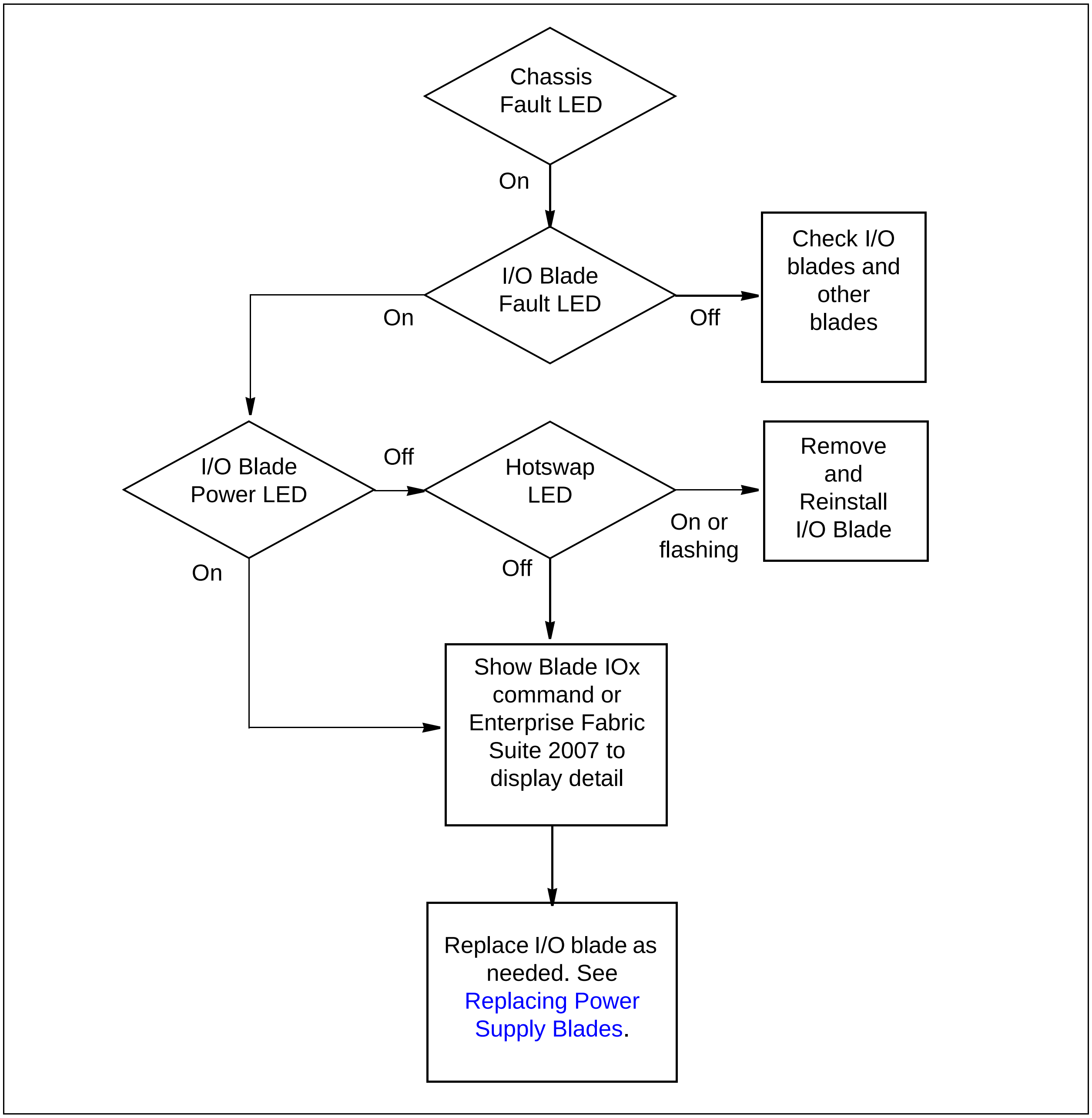

Chassis Fault LED
On
I/O Blade Fault LED
On
Off
Check I/O blades and other blades
I/O Blade Power LED
Off
Hotswap LED
Remove and Reinstall I/O Blade
On or flashing
On
Off
Show Blade IOx command or Enterprise Fabric Suite 2007 to display detail
Replace I/O blade as needed. See Replacing Power Supply Blades.

Figure 4-2 I/O Blade Diagnostic Process

FC Port Diagnostics

Port diagnostics for each port are indicated by the Logged-In LED. The Logged-In LED is the top LED of the pair to the right of each port on an I/O blade. For example, Figure 4-3 identifies the Logged-In LEDs for first four ports on an I/O blade.

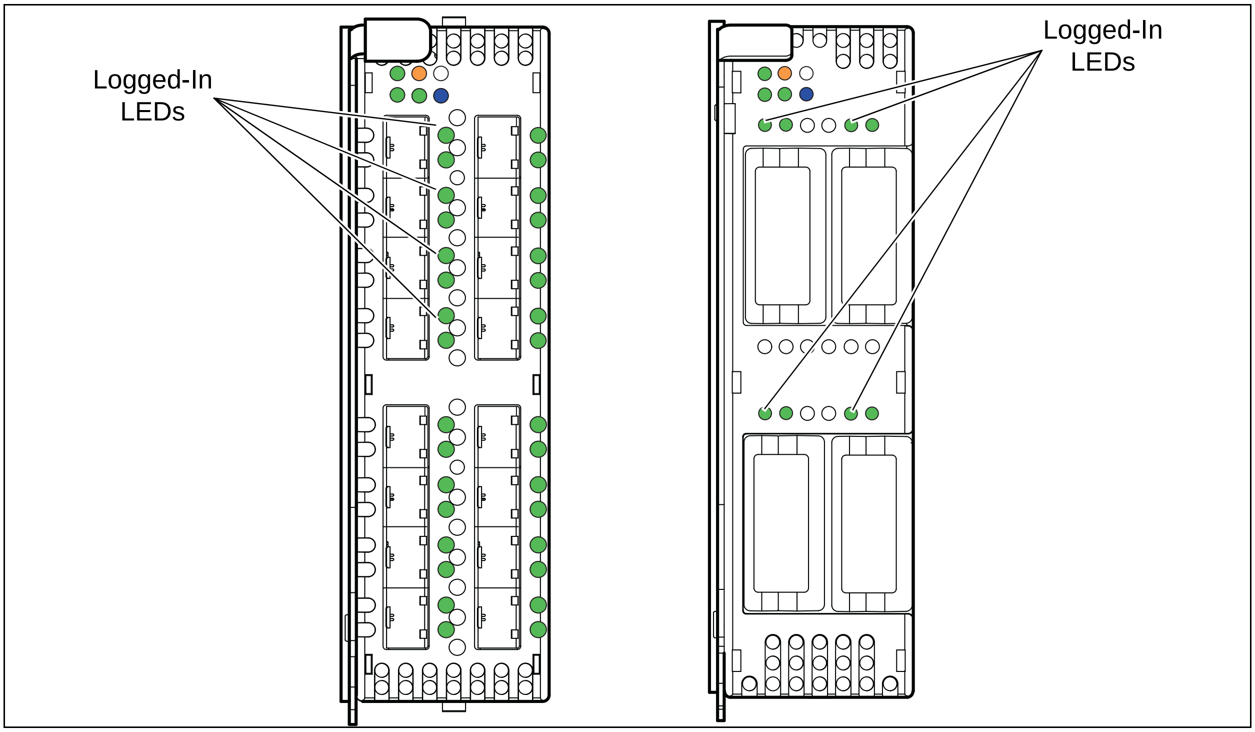


Figure 4-3 Logged-In LED

The Logged-In LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: The port is busy, or the port is in the diagnostics state.
- Flashing twice per second: The port is down, offline, or an error has occurred. This does not apply to a port that fails a diagnostic test.

If a Logged-In LED shows an error indication, review the event browser for alarm messages regarding the affected port. You can also inspect the event log using the Show Alarm command. Pertinent alarm messages will point to one or more of the following conditions:

- E_Port Isolation
- Excessive Port Errors

E_Port Isolation

A Logged-In LED error indication is often the result of E_Port isolation. An isolated E_Port is indicated by a red link in the Enterprise Fabric Suite 2007 topology display. E_Port isolation can be caused by the following:

- Security failure
- FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zone sets

Refer to the *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide* or the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about how to change domain IDs, timeout values, and edit zoning. Review the event browser and do the following to diagnose and correct an isolated E_Port:

1. Does the event browser show an invalid attach alarm for the affected port?
   - Yes - 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 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 command or the Switch data tab in the Enterprise Fabric Suite 2007 topology display. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command or the Enterprise Fabric Suite 2007 Switch Properties window. 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 command or the Switch data tab of the Enterprise Fabric Suite 2007 topology display. Are the timeout values the same?

   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch command or the Enterprise Fabric Suite 2007 Switch Properties dialog. Reset the port. If the condition remains, continue.

5. Display the active zone set on each switch using the Zoning Active command or the **Active Zoneset** tab of the Enterprise Fabric Suite 2007 topology display. Compare the zone membership between the two active zone sets. Are they the same?

   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. Reset the port. If the condition remains, contact your authorized maintenance provider.

   NOTE:

   This can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

Excessive Port Errors

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

- Device CRC errors
- Device decode errors
- Device ISL connection count
- Device login errors
- Device logout errors
- Device loss-of-signal errors

Port threshold alarm monitoring is disabled by default. Refer to the *SANbox 9000 Series Enterprise Fabric Suite 2007 User Guide* for information about managing port threshold alarms.

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
- Fault 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 do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command or a management application. 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. 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 - 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

NOTE:

Transceiver diagnostic information is available with purchase of the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider.

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.

Power Supply Blade Diagnostics

Figure 4-4 illustrates the Power Supply blade diagnostic process. If the corrective action is not successful, contact you authorized maintenance provider.

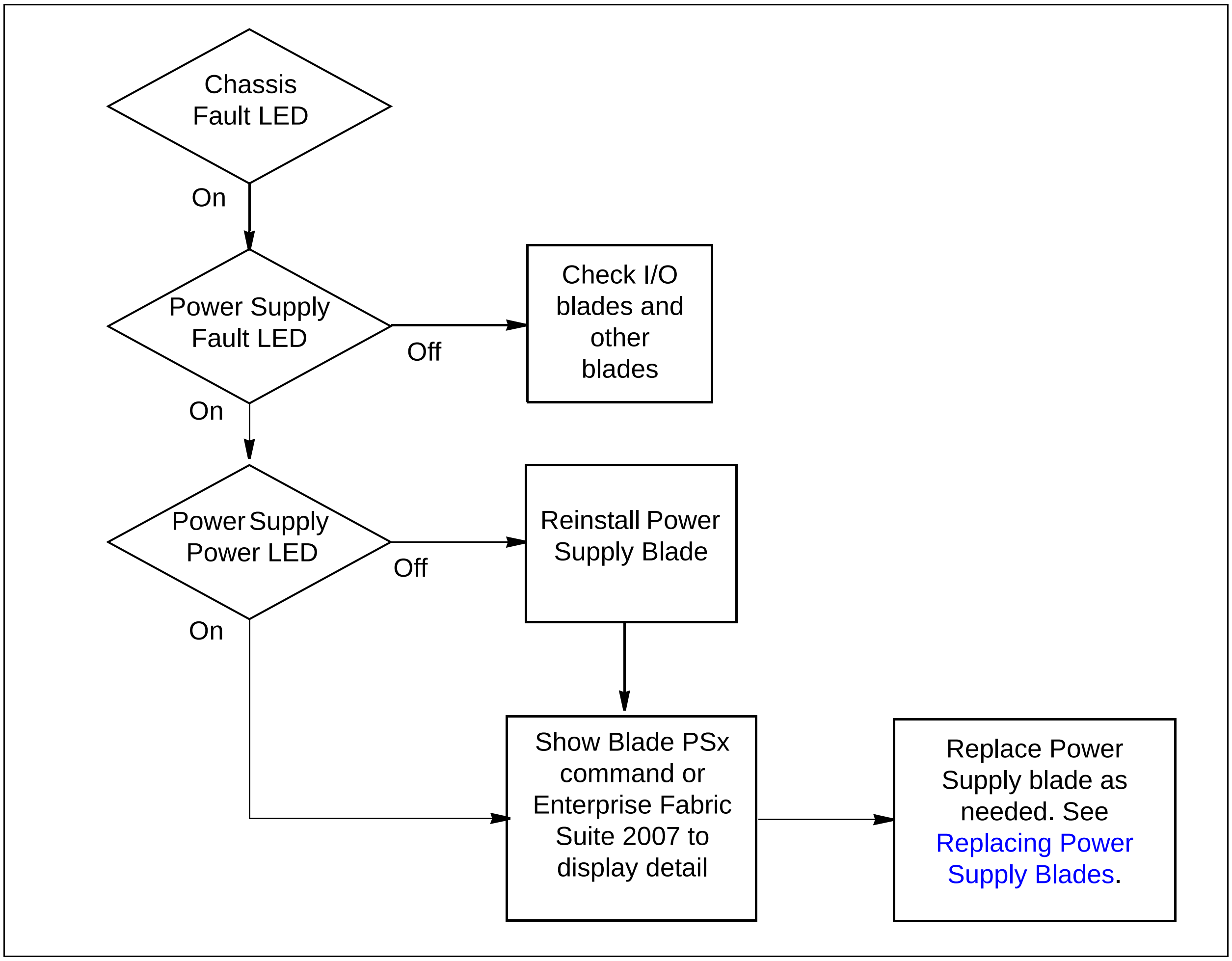

Chassis Fault LED
On
Power Supply Fault LED
Off
Check I/O blades and other blades
On
Power Supply Power LED
Off
Reinstall Power Supply Blade
On
Show Blade PSx command or Enterprise Fabric Suite 2007 to display detail
Replace Power Supply blade as needed. See Replacing Power Supply Blades.

Figure 4-4 Power Supply Blade Diagnostics Process

Fan Blade Diagnostics

Figure 4-5 illustrates the Fan blade diagnostic process. If the corrective action is not successful, contact you authorized maintenance provider.

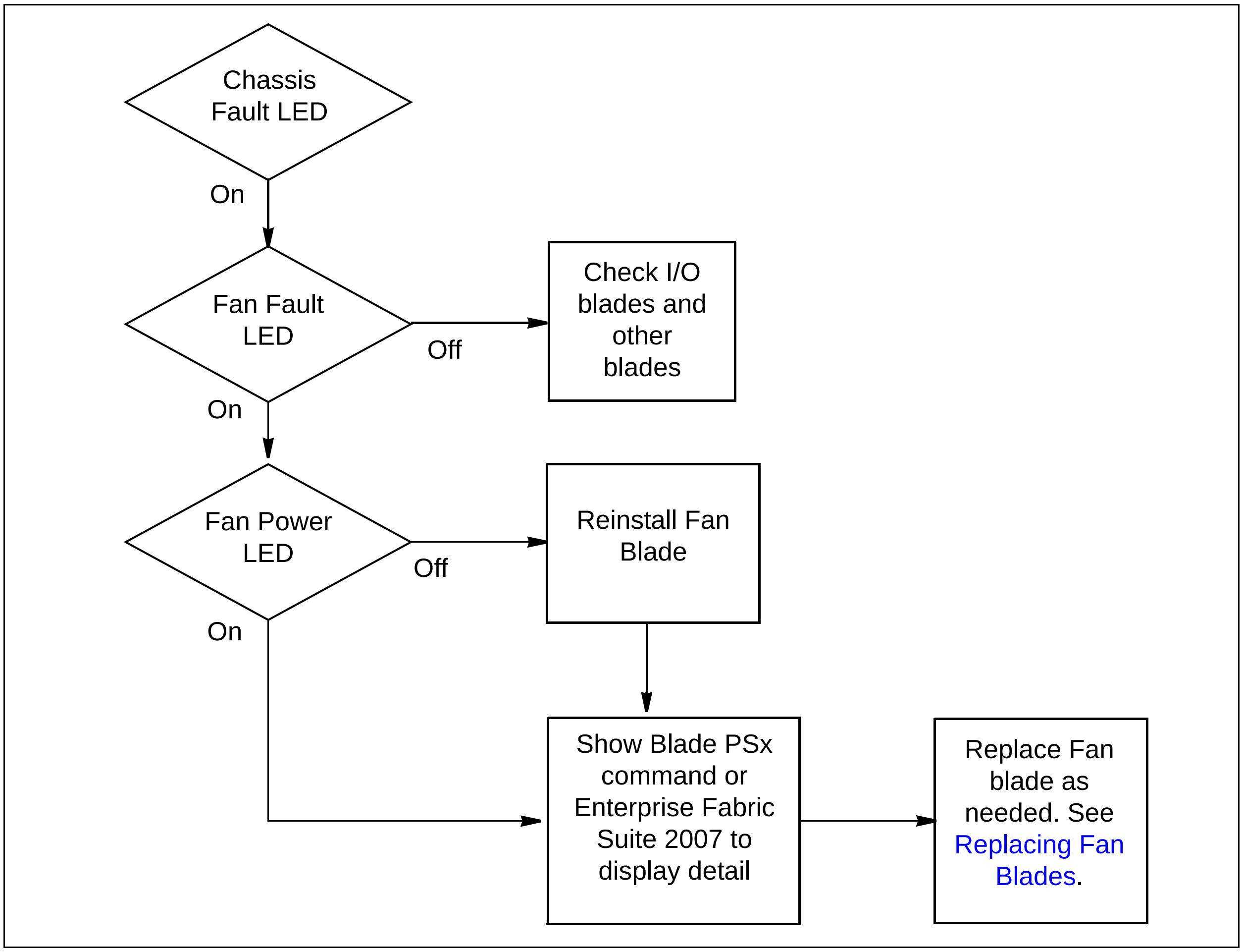

Chassis Fault LED
On
Fan Fault LED
Off
Check I/O blades and other blades
On
Fan Power LED
Off
Reinstall Fan Blade
On
Show Blade PSx command or Enterprise Fabric Suite 2007 to display detail
Replace Fan blade as needed. See Replacing Fan Blades.

Figure 4-5 Fan Blade Diagnostic Process

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
- Forgotten password

In these specific cases, you can recover the switch by placing the primary CPU blade in maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to perform the following tasks:

- Exiting the Maintenance Menu
- Unpacking a Firmware Image File
- Resetting the Network Configuration.
- Resetting User Accounts
- Copying Log Files
- Removing the Switch Configuration
- Remaking the File System\
- Resetting a Blade

To recover a switch, do the following:

1. Place the switch in maintenance mode. Refer to "Placing the Switch in Maintenance Mode" on page 1-11 for detailed instructions.
2. Allow one minute for the switch to complete its tests. When the switch is in maintenance mode, the Heartbeat LED will illuminate continuously.
3. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
4. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

```
Sanbox login: prom
Password:xxxx
Trying 10.0.0.1...
Connected to 10.0.0.1.
```

5. 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 the Enter key.

```
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 Blade
Option:
```

Exiting the Maintenance Menu

This option closes the current login and Telnet session. To log in again, enter the maintenance mode account name and password (prom, prom). To return to normal operation, power cycle the switch.

Unpacking a Firmware Image File

This 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 do the following:

1. Enter the FTP command and the switch IP address or symbolic name.

```
>ftp 10.0.0.1
```

2. When prompted for a user and password, enter the FTP account name and password (images, images).

```
user:images
password: images
```

3. Set binary mode and use the Put command to upload the firmware image file (7.8.xx.xx_ThCP).

```
ftp>put 7.8.xx.xx_ThCP
    xxxxx bytes sent in xx secs.
ftp>quit
```

4. Place the switch in maintenance mode. Refer to "Recovering a Switch Using Maintenance Mode" on page 4-15 for detailed instructions.

5. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
    telnet 10.0.0.1
```

6. Enter the maintenance mode account name and password (prom, prom), and press the Enter key.

   ```
   Sanbox login: prom
   Password:xxxx
   ```

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

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

8. Select option 7 to reset the switch and exit maintenance mode.

Resetting the Network Configuration

This option resets the network properties to the factory default values and saves them on the switch.

Resetting User Accounts

This 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

This option copies all log file buffers to a file on the switch named logfile. You can use FTP to download this file to the management workstation. You must download the logfile before resetting the switch. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about downloading files from the switch.

Removing the Switch Configuration

This option deletes all configurations from the switch except for the default configuration. This restores switch configuration parameters to the factory defaults except for user accounts and zoning.

Remaking the File System

In the event of sudden loss of power, it is possible that the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. This option resets the switch to the factory default values including user accounts and zoning.

CAUTION!

> 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 a Blade

This option resets the CPU blade.

5 Customer Replaceable Units

This section describes the removal and installation procedures for the following Customer Replaceable Units (CRU):

- Replacing Transceivers and Stacking Cables
- Replacing I/O Blades
- Replacing CPU Blades
- Replacing Power Supply Blades
- Replacing Fan Blades

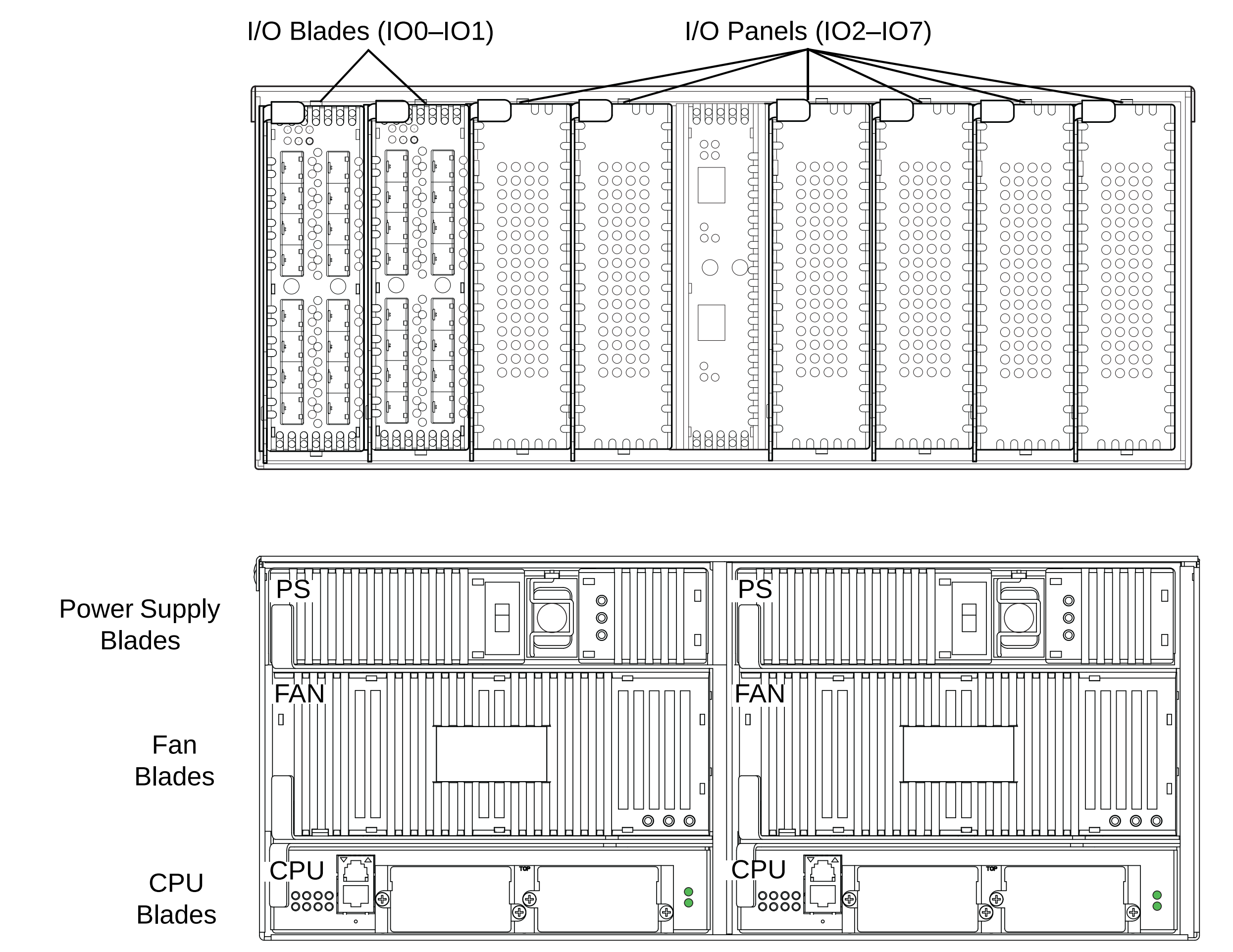


Figure 5-1 QLogic 9000 Series Customer Replaceable Units

CAUTION!

To prevent overheating, all blades and blank panels must be in place to provide proper cooling.

ATTENTION!

Afin de prévenir toute surchauffe, toutes les lames et tous les caches doivent rester en place pour assurer un refroidissement approprié.

VORSICHT!

Um Überhitzung zu verhindern, müssen alle Steckkarten und freien Fächer an der richtigen Stelle plaziert sein, damit eine einwandfreie Kühlung gewährleistet wird.

¡PRECAUCIÓN!

Para evitar un calentamiento excesivo, todas las placas y paneles vacíos deben estar en su sitio para proporcionar una refrigeración adecuada.

Replacing Transceivers and Stacking Cables

The transceivers and stacking cables can be removed and replaced while the switch is operating without damaging the switch or the transceiver. However, transmission on the affected port will be interrupted until the transceiver is installed and reconnected. To remove a transceiver, pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver. To install, insert the transceiver into the port and gently press until it snaps in place. The transceiver will fit only one way. If the transceiver does not install under gentle pressure, flip it over and try again.

Replacing CPU Blades

The following replacement procedures assume the use of the CLI. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about the CLI commands. Mechanically, these instructions also apply to removing and installing a CPU blade panel.

CAUTION!

> Always use an ESD wrist strap when removing and installing a CPU blade. The CPU blade contains sensitive logic components. To avoid damage to the blade, do not touch the CPU blade components. Keep the CPU blade in an ESD protective container or anti-static bag when not in use.

ATTENTION!

> Portez toujours un bracelet antistatique lors du retrait et de l'installation d'une lame d'unité centrale. Les lames d'unité centrale contiennent des composants logiques sensibles. Pour éviter d'endommager la lame, ne touchez pas les composants de lame d'unité centrale. Lorsque vous ne l'utilisez pas, conservez la lame d'unité centrale dans un conteneur ou un sachet antistatique.

VORSICHT!

> Benutzen Sie immer ein ESD-Handgelenkband, wenn Sie ein CPU-Steckkarte entfernen und installieren. Die CPU-Steckkarte umfasst empfindliche Steuerkomponenten. Um Beschädigungen der Steckkarte zu verhindern, fassen Sie die Komponenten der CPU-Steckkarte nicht an. Lassen Sie die CPU-Steckkarte in einem ESD-Schutzcontainer oder Antistatikbeutel, wenn sie nicht benutzt wird.

¡PRECAUCIÓN!

> Utilice siempre una muñequera antiestática cuando elimine e instale una placa CPU. La placa CPU contiene componentes lógicos sensibles. Para evitar dañar la placa, no toque los componentes de la placa CPU. Guarde la placa CPU en un contenedor protector ESD o en una bolsa antiestática cuando no se utilice.

The CPU blade replacement process depends on the following factors:

- Licensing: standard or fault tolerant
- Single or dual CPU blade switch
- CPU blade type: primary or secondary

The CPU blade replacement procedures are as follows:

- Standard Single CPU – Primary CPU Blade Replacement
- Standard Dual CPU – Primary CPU Blade Replacement
- Fault Tolerant – Primary CPU Blade Replacement
- Secondary CPU Blade Replacment

WARNING!!

The CPU blade heat sinks can become very hot. Handle with care.

AVERTISSEMENT!!

Les dissipateurs de chaleur des lames de l'unité centrale peuvent devenir très chauds. Manipulez-les avec précaution.

WARNUNG!!Das CPU-Wärmeableitblech kann sehr heiß werden. Lassen Sie Vorsicht walten.

¡ADVERTENCIA!

Los disipadores de calor de la placa CPU pueden estar muy calientes. Manipúlelos con cuidado.

Standard Single CPU – Primary CPU Blade Replacement

For a standard, single CPU blade switch, the primary CPU blade can be CPU0 or CPU1.

1. Determine the firmware version. Open a Telnet session and enter the Show Version CLI command to determine the current firmware version. Make note of the firmware version. If the switch is inaccessible, obtain the firmware version from another switch in the fabric or from your records.
2. Configure the Telnet window to log output to a file. Enter the Show Support command to document the switch and capture the output on a file.
3. Back up the switch configuration. Enter the Config Backup command to back up the switch configuration to a file on the switch named *configdata*.
4. Back up the event log. Enter the Set Log Archive command to back up the event log to a file on the switch named *logfile*.
5. Download the configuration and log files to your workstation. Open an FTP session to download the *configdata* and *logfile* files onto your workstation. Later, you will restore the switch configuration using the *configdata* file.

   ```
   ftp <ip_address>
   User: images
   Password: images
   ftp> binary
   ftp> get configdata
   ftp> get logfile
   ftp> bye
   ```

6. Disconnect the cables from the CPU blade Ethernet and serial ports.
7. Open the latch fully and pull the CPU blade by the latch to disengage the blade as shown in Figure 5-2.

WARNING!!

The CPU blade heat sinks can become very hot. Handle with care.

AVERTISSEMENT!!

Les dissipateurs de chaleur des lames de l'unité centrale peuvent devenir très chauds. Manipulez-les avec précaution.

WARNUNG!!Das CPU-Wärmeableitblech kann sehr heiß werden. Lassen Sie Vorsicht walten.

¡ADVERTENCIA!

Los disipadores de calor de la placa CPU pueden estar muy calientes. Manipúlelos con cuidado.

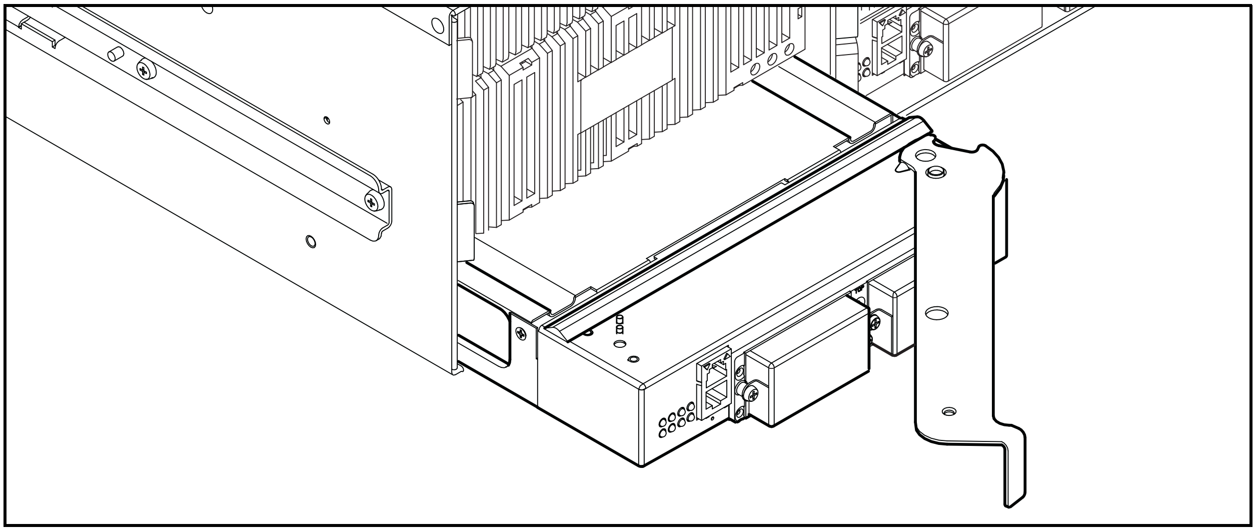


Figure 5-2 Removing the CPU0 Blade

8. Install the new CPU blade. Remove protective coverings from the backplane connectors. Open the CPU blade latch and slide the blade into the chassis until it makes contact with the midplane connector. Rotate the latch to lock the CPU blade in place. When the CPU blade is properly installed, the Hotswap LED will be extinguished.

9. Reconnect cables to the Ethernet and serial ports. The IP address of a factory CPU blade replacement is 10.0.0.1.

10. Observe the CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, contact your authorized maintenance provider.

11. Verify the POST results. Open a Telnet session with the default IP address (10.0.0.1), and enter the Show Blade CPU command to display the diagnostic status for the CPU blade.

12. Compare firmware versions. Open a Telnet session and enter the Show Version command to determine the firmware version.

    - If the firmware versions are different, proceed to Step 13 to restore the switch configuration.

    - If the firmware versions on the old and new CPU blades are the same, proceed to Step 16 to restore the switch configuration.

13. Install firmware. Acquire the firmware image file from your own storage or you can download firmware from the QLogic web site.

14. Load the image file on the switch. Move to the directory that contains the firmware image file and open an FTP session. When prompted, enter the account name (images) and password (images). Set the file type to binary. Enter the Put command and specify the name of the image file.

    ```
    ftp 10.0.0.1
    User: images
    Password: images
    ftp> binary
    ftp> put image_file
    ftp> bye
    ```

15. Log in to the switch with the default user name (admin) and password (password). Open an Admin session and enter the Image Unpack command. Enter the Reset command to activate the new firmware. End the Admin session and log off.

    ```
    Telnet 10.0.0.1
    CPU0 login: admin
    Password: password

    SANbox #> admin start
    SANbox (admin) #> image unpack image_file
    Image unpack command result: Passed
    SANbox (admin) #> reset
    SANbox (admin) #> admin end
    SANbox #> exit
    ```

16. Move to the directory that contains the *configdata* file that you downloaded earlier. Use FTP to upload this file from the management workstation to the switch.

    ```
    ftp 10.0.0.1
    User: images
    Password: images
    ftp> binary
    ftp> put configdata
    ftp> bye
    ```

17. Restore the switch configuration. Log in to the switch again and open a Telnet session. Enter the Config Restore command to restore the switch configuration. When the switch resets, the Telnet session will terminate.

    ```
    Telnet 10.0.0.1
    CPU0 login: admin
    Password: password

    SANbox #> admin start
    SANbox (admin) #> config restore
    The switch will be reset after restoring the
    configuration.
      Please confirm (y/n): [n] y
    ```

18. Log in to the switch again using the original IP address.

19. Observe the CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to diagnostic procedures in the installation guide, or contact your authorized maintenance provider.

Standard Dual CPU – Primary CPU Blade Replacement

For a standard, dual CPU blade switch, the primary CPU blade can be CPU0 or CPU1. Because the switch is not licensed for fault tolerance, control does not transfer to the secondary CPU blade without shutting down the switch and removing the primary CPU blade. When the switch is powered up again, the the secondary switch becomes primary. After the new CPU blade is installed, the firmware and switch configuration will be restored to the new CPU blade automatically.

You can determine the primary CPU by locating the illuminated CPU Primary LED. You can also determine the primary CPU blade, by entering the Show Blade command and looking for the “+” opposite the primary CPU blade.

1. Turn the On/Off switches on both Power Supply blades to the Off position.

2. Disconnect the Ethernet, serial, and HyperStack cables from the primary CPU blade.

3. Open the latch fully and pull the CPU blade by the latch to disengage the blade from the midplane.

4. Turn the On/Off switches on both Power Supply blades to the On position. When the switch becomes operational, the former secondary CPU will become primary.

5. Observe the new primary CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to diagnostic procedures in the installation guide, or contact your authorized maintenance provider.
6. Install the new secondary CPU blade. Remove protective coverings from the backplane connectors. Open the CPU blade latch and slide the CPU blade into the chassis until it makes contact with the midplane connector. Rotate the latch to lock the CPU blade in place. When the switch becomes operational, the firmware and switch configuration will automatically transfer to the new CPU blade. Upgrading firmware will take a few minutes and complete by resetting the CPU blade.
7. Reconnect the Ethernet, serial port, and HyperStack cables.
8. Log in to the switch again using the original IP address.
9. Observe the CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to "Error Code Blink Patterns" on page 4-2 for diagnostic information.
10. Verify the POST results. Open a Telnet session and enter the Show Blade command to display the diagnostic status for the CPU blade.

Fault Tolerant – Primary CPU Blade Replacement

With a switch that is licensed for Fault Tolerance, you can transfer control to the secondary CPU blade, then remove the primary CPU blade; or simply remove the primary CPU blade while the switch is running–control transfers automatically.

You can determine the primary CPU by locating the illuminated CPU Primary LED. You can also determine the primary CPU blade, by entering the Show Blade command and looking for the "+" opposite the primary CPU blade.

1. Enter the Show Version command to verify that SecondaryCPUStatus is HotStandby. Control will not transfer unless the secondary CPU status is HotStandby.

   Optional: Enter the Switchover CLI command to explicitly transfer control to the secondary CPU blade, then proceed to "Secondary CPU Blade Replacment" on page 5-11. Otherwise, proceed to Step 2.
2. Disconnect the Ethernet, serial, and HyperStack cables from the primary CPU blade.
3. Rotate the latch to the partial open position until the blue Hotswap LED begins flashing. Wait for the Hotswap LED to illuminate continuously, then open the latch fully and pull the CPU blade by the latch to disengage the blade from the midplane. The secondary CPU blade automatically becomes primary.

4. Install the new CPU blade. Remove protective coverings from the backplane connectors. Open the CPU blade latch and slide the blade into the chassis until it makes contact with the midplane connector. Rotate the latch to lock the CPU blade in place. When the CPU blade is properly installed, the blue Hotswap LED will be extinguished.
5. Reconnect the Ethernet, serial port, and HyperStack cables.
6. The new CPU blade is secondary and receives firmware and configuration information from the primary CPU blade.
7. Observe the CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to "Error Code Blink Patterns" on page 4-2 for diagnostic information.
8. Verify the POST results. Open a Telnet session with the default IP address, and enter the Show Blade command to display the diagnostic status for the CPU blade.

Secondary CPU Blade Replacment

The secondary CPU blade can be CPU0 or CPU1 and can be removed without disrupting switch operation with or without the Fault Tolerant license. You can determine the secondary CPU by locating the extinguished CPU Primary LED. You can also determine the secondary CPU blade, by entering the Show Blade command and looking for the CPUx entry without the "+".

1. Disconnect the Ethernet, serial, and HyperStack cables from the secondary CPU blade.
2. Rotate the latch to the partial open position until the blue Hotswap LED begins flashing. Wait for the Hotswap LED to illuminate continuously, then open the latch fully and pull the CPU blade by the latch to disengage the blade from the midplane.
3. Install the new CPU blade. Remove protective coverings from the backplane connectors. Open the CPU blade latch and slide the CPU blade into the chassis until it makes contact with the midplane connector. Rotate the latch to lock the CPU blade in place. When the CPU blade is properly installed, the blue Hotswap LED will be extinguished.
4. Reconnect the Ethernet, serial port, and HyperStack cables. When the switch becomes operational, the firmware and switch configuration will automatically transfer to the new CPU blade.
5. Observe the CPU blade Heartbeat LED. It should blink once per second. If the Heartbeat LED is showing a different blink pattern, refer to "Error Code Blink Patterns" on page 4-2 for diagnostic information.
6. Verify the POST results. Open a Telnet session and enter the Show Blade command to display the diagnostic status for the CPU blade.

Replacing I/O Blades

You can remove and install I/O blades while the switch is operating. The following instructions assume that the switch is operating. If you want to maintain service to the devices connected to a particular blade while it is being replaced, transfer the Fibre Channel cables to another I/O blade. Mechanically, these instructions also apply to removing and installing a I/O blade blank panel.

The following removal and installation procedures describe how to remove an I/O blade using the CLI. Refer to the *SANbox 9000 Series Stackable Chassis Switch Command Line Interface Guide* for information about the CLI commands.

CAUTION!

Always use an ESD wrist strap when removing and installing an I/O blade. An I/O blade contains sensitive logic components. Keep the I/O blade in an ESD protective container or anti-static bag when not in use.

ATTENTION!

Portez toujours un bracelet antistatique lors du retrait et de l'installation d'une lame d'E/S. Les lames d'E/S contiennent des composants logiques sensibles. Lorsque vous ne l'utilisez pas, conservez la lame d'E/S dans un conteneur ou un sachet antistatique.

VORSICHT!

Benutzen Sie immer ein ESD-Handgelenkband, wenn Sie eine E/A-Steckkarte entfernen oder installieren. Eine E/A-Steckkarte enthält empfindliche Steuerkomponenten. Bewahren Sie die E/A- Steckkarte in einem ESD-Schutzcontainer oder Antistatikbeutel auf, wenn sie nicht benutzt wird.

¡PRECAUCIÓN!

Utilice siempre una muñequera antiestática cuando elimine e instale una placa de E/S. Una placa de E/S contiene componentes lógicos sensibles. Guarde la placa de E/S en un contenedor protector ESD o en una bolsa antiestática cuando no se utilice.

Removing an I/O Blade

CAUTION!

To avoid overheating, do not operate the switch with an empty I/O slot any longer than it takes to install a new I/O blade.

ATTENTION!

Pour éviter toute surchauffe, ne faites pas fonctionner le commutateur avec un emplacement d'E/S vide plus longtemps que nécessaire pour installer une nouvelle lame d'E/S.

VORSICHT!

Um Überhitzung zu verhindern, lassen Sie den Switch mit einem leeren E/A-Steckplatz nicht länger in Betrieb sein, als eine Installation einer neuen E/A-Steckkarte dauert.

¡PRECAUCIÓN!

Para evitar un calentamiento excesivo, no utilice el conmutador con una ranura de E/S vacía durante más tiempo del que se tarda en instalar una placa de E/S nueva.

To remove an I/O blade, do the following:

1. Label and disconnect the Fibre Channel port cables. Label Fibre Channel port cables by port number.
2. Open a Telnet session and enter the Set Blade command to place the I/O blade in the powered-off state. Observe that the blue Hotswap LED is illuminated. The Hotswap LED illuminates continuously to indicate that power to the blade has ceased and the blade can be removed.
3. Pull the I/O blade by the latch to disengage the I/O blade from the midplane as shown in Figure 5-3. Carefully slide the I/O blade out of the chassis.

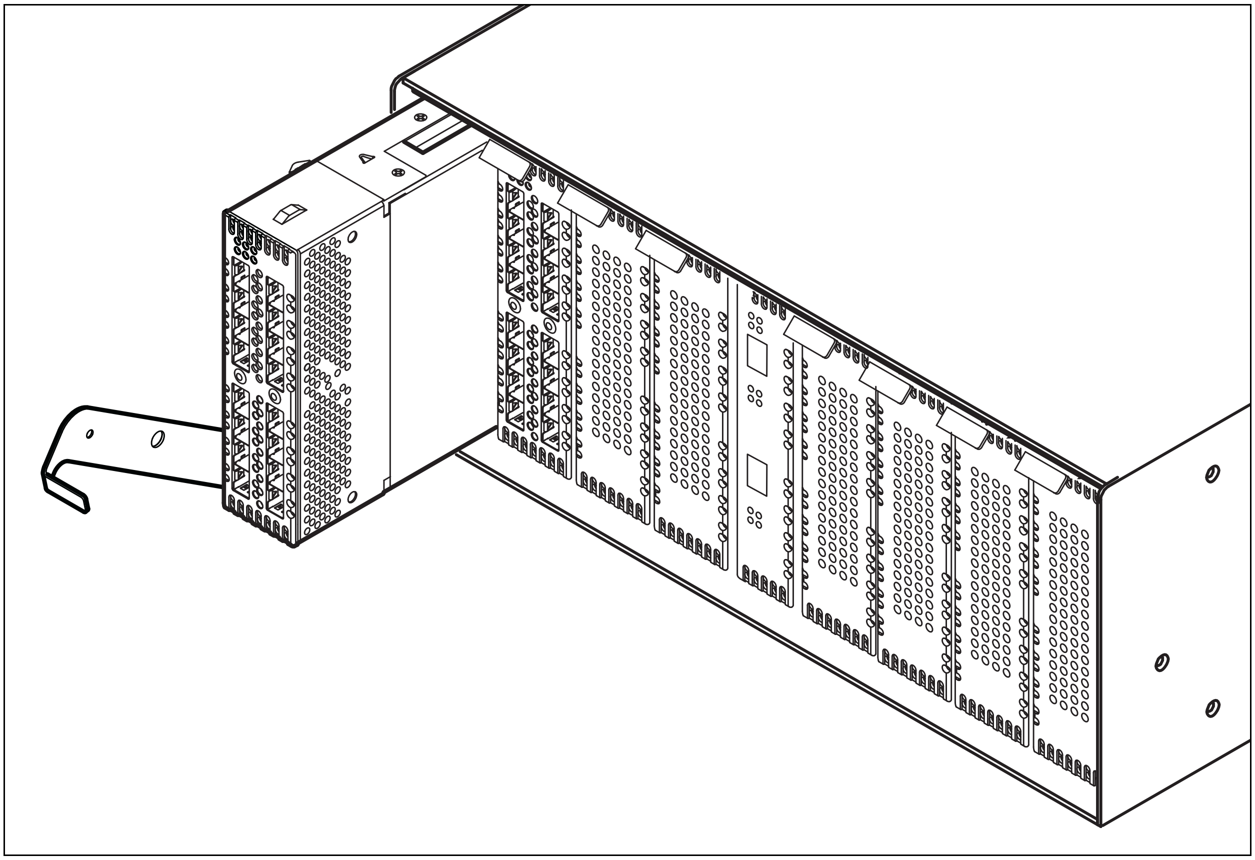


Figure 5-3 Removing an I/O Blade

Installing an I/O Blade

NOTE:

8-Gbps I/O blades require firmware version 7.8 or higher.

To install an I/O blade, do the following:

1. Open the I/O blade latch and slide the I/O blade into the chassis until it makes contact with the midplane connector.
2. Rotate the latch upward to lock the I/O blade in place. When the I/O blade is properly installed, the Hotswap LED will extinguish. If the Hotswap LED begins flashing, remove the I/O blade and reinstall it.
3. Confirm the I/O blade status. Open a Telnet session and enter the Show Chassis command to display the operational status of the I/O blade.
4. Reconnect the Fiber Channel port cables according to their labels.

Replacing Power Supply Blades

You can remove or install one of the two functioning power supply blades without disrupting service. The Power Supply blades are interchangeable; that is, a Power Supply blade will fit in any bay. Power Supply blades can have front-to-back or back-to-front air flow; however both Power Supply blades and Fan blades must have the same air flow direction.

WARNING!!

The Power Supply blade faceplate and internal surfaces can become very hot. Handle with care.

Voltage is present in an open slot when the switch is operating. To avoid personal injury or damage to surrounding components, do not place hands or objects into an open slot.

AVERTISSEMENT!!

La plaque frontale du module d'alimentation et des surfaces internes peuvent s'échauffer très rapidement. Manipuler avec précaution.

Lorsque le commutateur est en marche, la rainure ouverte est sous tension. Pour éviter toute blessure personnelle ou dommage aux composants environnants, ne pas placer les mains ou des objets dans une rainure ouverte.

WARNUNG!!

Die Frontabdeckung des Stromversorgungsmoduls und die Innenoberflächen können sehr heiß werden. Vorsichtig behandeln.

In einem offenen Steckplatz ist Spannung vorhanden, wenn der Switch in Betrieb ist. Zur Vermeidung von Verletzung oder Beschädigung von Komponenten in der Umgebung weder die Finger noch irgendwelche Objekte in einen offenen Steckplatz einführen.

¡ADVERTENCIA!

La placa frontal de la placa de suministro de energía y las superficies internas pueden estar muy calientes. Manipúlelas con cuidado.

Cuando el conmutador funciona, hay tensión eléctrica en las ranuras abiertas. Para evitar lesiones personales o daños en los componentes cercanos, no ponga las manos ni ningún objeto en una ranura abierta.

CAUTION!

Always use an ESD wrist strap when removing and installing a Power Supply blade. A Power Supply blade contains sensitive logic components. Keep the Power Supply blade in an ESD protective container or anti-static bag when not in use.

To avoid overheating, do not operate the switch with an empty Power Supply blade slot any longer than it takes to install a new Power Supply blade.

Replacement Power Supply blades must be compatible with the switch air flow direction of the other Power Supply blade and Fan blades. Installing a Power Supply blade with an opposing air flow direction could lead to overheating.

ATTENTION!

Portez toujours un bracelet antistatique lors du retrait et de l'installation d'une lame de bloc d'alimentation. Les lames de bloc d'alimentation contiennent des composants logiques sensibles. Lorsque vous ne l'utilisez pas, conservez la lame de bloc d'alimentation dans un conteneur ou un sachet antistatique.

Pour éviter toute surchauffe, ne faites pas fonctionner le commutateur avec un emplacement de lame de bloc d'alimentation vide plus longtemps que nécessaire pour installer une nouvelle lame de bloc d'alimentation.

La direction du flux d'air des lames de bloc d'alimentation de rechange doit être compatible avec celle des autres lames de bloc d'alimentation et de ventilateur. L'installation d'une lame de bloc d'alimentation dont la direction du flux d'air est opposée à celle des autres flux pourrait entraîner une surchauffe.

VORSICHT!

Benutzen Sie immer ein ESD-Handgelenkband, wenn Sie eine Netzteilsteckkarte entfernen und installieren. Eine Netzteilsteck- karte umfasst empfindliche Steuerkomponenten. Lassen Sie die Netzteilsteckkarte in einem ESD-Schutzcontainer oder Antistatik- beutel, wenn sie nicht benutzt wird.

Um Überhitzung zu verhindern, lassen Sie den Switch mit einem leeren Netzteilsteckplatz nicht länger in Betrieb sein, als die Instal- lation einer neuen Netzteilsteckkarte dauert.

Ersatz-Netzteilsteckkarten müssen mit der Switch-Luftströmungs- richtung der anderen Netzteilsteckkarte und Lüftungssteckkarten kompatibel sein. Wenn Sie eine Netzteilsteckkarte mit einer gegen- sätzlichen Luftströmungsrichtung installieren, könnte das zur Über- hitzung führen.

¡PRECAUCIÓN!

Utilice siempre una muñequera antiestática cuando elimine e instale una placa de suministro de energía. Una placa de suministro de energía contiene componentes lógicos sensibles. Guarde la placa de suministro de energía en un contenedor protector ESD o en una bolsa antiestática cuando no se utilice.

Para evitar un calentamiento excesivo, no utilice el conmutador con una ranura de placa de suministro de energía vacía durante más tiempo del que se tarda en instalar una placa de suministro de energía nueva.

Las placas de suministro de energía de repuesto deben ser compatibles con la dirección del flujo de aire del conmutador de la otra placa de suministro de energía y las placas del ventilador. La instalación de una placa de suministro de energía con un flujo de aire en dirección opuesta podría producir un calentamiento excesivo.

Removing a Power Supply Blade

To remove a power supply blade, do the following:

1. Confirm that the primary CPU Heartbeat LED is showing the normal 1 blink per second. This allows the switch to correctly report power supply status.
2. Move the Power Supply blade On/Off switch to the off position.
3. Unfasten the bail from the plug and unplug the cord from the Power Supply blade.
4. Rotate the latch to the full open position. Pull the Power Supply blade by the latch to disengage the blade from the midplane connector as shown in Figure 5-4. Carefully slide the Power Supply blade out of the chassis.

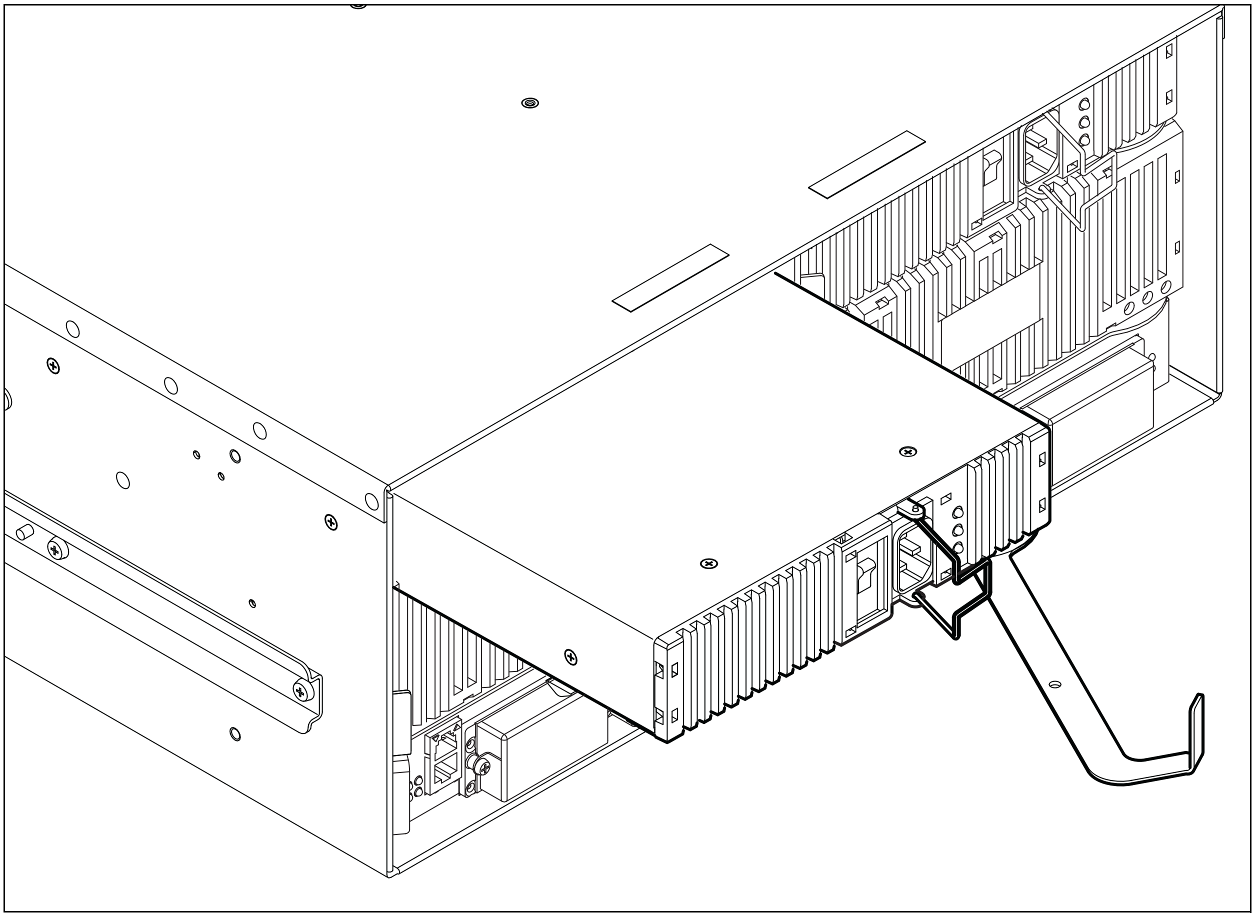


Figure 5-4 Removing a Power Supply Blade

Installing a Power Supply Blade

To install a Power Supply blade, do the following:

1. Confirm that the CPU blade Heartbeat LED is showing the normal 1 blink per second. This allows the switch to correctly report power supply status.
2. Open the Power Supply blade latch and slide the blade into the chassis until it contacts the midplane connector.
3. Rotate the latch right-to-left to lock the Power Supply blade in place.
4. Move the Power Supply blade On/Off switch to the On position. Observe that the Power Supply blade Power LED is illuminated.
5. Confirm the Power Supply blade status. Open a Telnet session and enter the Show Chassis command to display the operational status of the Power Supply blade.

Replacing Fan Blades

You can remove or install one of the Fan blades while the switch is operating without disrupting service. The Fan blades are also interchangeable; that is, a Fan blade will fit in any bay. Fan blades can have front-to-back or back-to-front air flow; however both Fan blades and Power Supply blades must have the same air flow direction.

WARNING!!

Voltage is present in an open bay when the switch is operating. To avoid personal injury, do not place hands or objects into an open bay.

AVERTISSEMENT!!

Lorsque le commutateur est en marche, la baie ouverte est sous tension. Pour éviter toute blessure personnelle, ne pas placer les mains ou des objets dans une baie ouverte.

WARNUNG!!In einem offenen Gestell ist Spannung vorhanden, wenn der Switch in Betrieb ist. Zur Vermeidung von Verletzung weder die Finger noch irgendwelche Objekte in ein offenes Gestell einführen.

¡ADVERTENCIA!

Cuando el conmutador funciona, hay tensión eléctrica en los compartimentos abiertos. Para evitar lesiones personales, no ponga las manos ni ningún objeto en un compartimento abierto.

CAUTION!

Always use an ESD wrist strap when removing and installing a Fan blade. Keep the Fan blade in an ESD protective container or anti-static bag when not in use.

Replacement Fan blades must be compatible with the air flow direction of the other Fan blade and Power Supply blades. Installing a Fan blade with an opposing air flow direction could lead to overheating.

To avoid overheating, do not operate the switch with an empty Fan blade slot any longer than it takes to install a new Fan blade.

ATTENTION!

Portez toujours un bracelet antistatique lors du retrait et de l'installation d'une lame de ventilateur. Lorsque vous ne l'utilisez pas, conservez la lame de ventilateur dans un conteneur ou un sachet antistatique.

La direction du flux d'air des lames de ventilateur de rechange doit être compatible avec celle des autres lames de ventilateur et de bloc d'alimentation. L'installation d'une lame de ventilateur dont la direction du flux d'air est opposée à celle des autres flux pourrait entraîner une surchauffe.

Pour éviter toute surchauffe, ne faites pas fonctionner le commutateur avec un emplacement de lame de ventilateur vide plus longtemps que nécessaire pour installer une nouvelle lame de ventilateur.

VORSICHT!

Benutzen Sie immer ein ESD-Handgelenkband, wenn Sie eine Lüftungssteckkarte entfernen und installieren. Lassen Sie die Lüftungssteckkarte in einem ESD-Schutzcontainer oder Antistatikbeu- tel, wenn er nicht benutzt wird.

Ersatz-Lüftungssteckkarten müssen mit der Switch-Luftströmungs- richtung der anderen Lüftungssteckkarte und der Netzteilsteck- karten kompatibel sein. Wenn Sie eine Lüftungssteckkarte mit einer gegensätzlichen Luftströmungsrichtung installieren, könnte das zur Überhitzung führen.

Um Überhitzung zu verhindern, lassen Sie den Switch mit einem leeren Lüftungssteckkartenplatz nicht länger in Betrieb sein, als die Installation einer neuen Lüftungssteckkarte dauert.

¡PRECAUCIÓN!

Utilice siempre una muñequera antiestática cuando elimine e instale una placa de ventilador. Guarde la placa de ventilador en un contenedor protector ESD o en una bolsa antiestática cuando no esté en uso.

Las placas de ventilador de repuesto deben ser compatibles con la dirección del flujo de aire del conmutador de la otra placa de ventilador y las placas de suministro de energía. La instalación de una placa de ventilador con un flujo de aire en dirección opuesta podría producir un calentamiento excesivo.

Para evitar un calentamiento excesivo, no utilice el conmutador con una ranura de placa de ventilador vacía durante más tiempo del que se tarda en instalar una placa de ventilador nueva.

Removing a Fan Blade

To remove a Fan blade, rotate the latch to the full open position. Pull the Fan blade by the latch to disengage the blade from the midplane connector as shown in Figure 5-5. Carefully slide the Fan blade from the chassis.

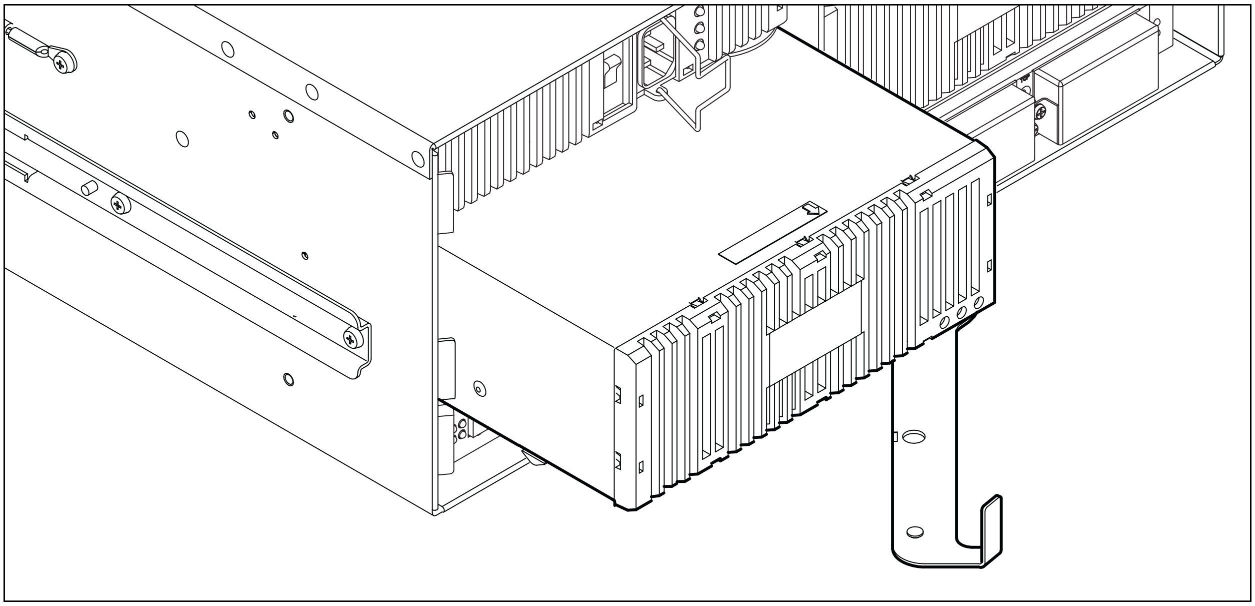


Figure 5-5 Removing a Fan Blade

Installing a Fan Blade

To install a Fan blade, do the following:

1. Open the Fan blade latch and slide the blade into the chassis until it contacts the midplane connector.
2. Rotate the latch right-to-left to lock the Fan blade in place.
3. Observe that the Fan blade Power LED is illuminated.
4. Confirm the Fan blade status. Open a Telnet session and enter the Show Chassis command to display the operational status of the Fan blade

Notes

A Specifications

This appendix contains the specifications for the QLogic 9000 Series switch. Refer to Section 1 for the location of all connections, switches, controls, and components.

Fabric Specifications

Table A-1. Fabric Specifications

Fibre Channel Protocols.................	FC-PI-3 FC-LS FC-FS-2 FC-GS, -2,-3, -4, -5 FC-SW-2, -3, -4 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-FLA FC-Tape FC-VI Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0 FC-MI-2 FC-DA FC-SP
Fibre Channel Classes of Service ..	Classes 2, 3, and F
Modes of Operation........................	Fabric Public loop Broadcast

Optional License Keys

Table A-2. Optional License Keys

SANdoctor	Supports Fibre Channel connection verification, Fibre Channel route tracing, and transceiver diagnostic information.
HyperStack	Supports the connection of two 9000 Series switches through the multiple 10-Gbps link Inter-Chassis Connectors (ICC).

Table A-2. Optional License Keys

Fault Tolerant	Supports automatic and manual failover of switch management functions from the primary CPU blade to the secondary CPU blade.

Performance Features

Table A-3. Performance Features

Fabric Port Speed	
■ 4-Gbps I/O Blades	1.0625, 2.125, 4.250-Gbps
■ 8-Gbps I/O Blades	2.125, 4.250, 8.50-Gbps
■ 10-Gbps I/O Blades	12.75-Gbps
Fabric Latency (best case)	
■ 4-Gbps I/O blade	<0.3 µsec @ 4-Gbps
■ 8-Gbps I/O blade	<0.2 µsec @ 8-Gbps
■ 10-Gbps I/O blade	<0.2 µsec @ 10-Gbps
Fabric Point-to-Point Bandwidth	212 MB, full duplex @ 1-Gbps
	424MB full duplex @ 2-Gbps
	850 MB full duplex @ 4-Gbps
	1700 MB full duplex @ 8-Gbps
	2550 MB full duplex @ 10-Gbps
System Bandwidth	
Backplane switching capacity	
■ Model 9100	408 Gbps, full duplex
■ Model 9200	816 Gpbs, full duplex
■ 2 x Model 9200 HyperStack	1632 Gpbs, full duplex; Non-blocking HyperStack architecture
Local switching capacity	
■ One 4-Gbps I/O blade	1088 Gbps
■ Two 4-Gbps I/O blades	2176 Gbps
■ One 8-Gbps I/O blade	2176 Gbps
■ Two 8-Gbps I/O blades	4352 Gbps
Maximum Frame Size	2148 bytes (2112 byte payload)

Table A-3. Performance Features

Per Port Buffering	■ ASIC-embedded memory (non-shared). ■ Each port has a guaranteed 16-credit zero wait state buffer for full performance up to 13Km @ 2-Gbps and 2 Km @ 10-Gbps ■ Buffer credit donor support software to extend distances
ISL Trunking	■ Up to 128 ISLs in one or more trunks between multiple switches in any port speed combination and across multiple I/O blades ■ Switch-On-Exchange (SOE) mode for dynamic ISL trunk load balancing to maximize throughput ■ In-order delivery of frames in all multi-switch and multi-link configurations ■ Automatic configuration of ISL trunks including multi-hop paths between multiple switches including stack, cascade, cascaded loop, and mesh ■ Adaptive trunking and intelligent path selection on all 10-Gbps ports ■ Non-disruptive dynamic addition of ISLs to an existing trunk ■ High availability with automatic path failover
System Processor	800 MHz PowerPC®
I/O blade Processor	400 MHz PowerPC

Modular Scalability

Table A-4. Modular Scalability

Ports per Chassis	■ 16 to 128 SFP ports ■ 4 to 32 X2 ports ■ Full blade intermix support, maximum 8 I/O blades, all blades hot-pluggable ■ >475,000 user ports depending on configuration
Ports Per Rack	Up to 1,280 ports per 42U rack
Chassis HyperStack	Supports high bandwidth interconnections between two Model 9200 switches using the HyperStack license and HyperStack cables.
Multi-switch Fabrics	■ Supports all topologies, including: stack, cascade, cascaded loop, and mesh ■ Maximum 239 switches depending on configuration
Fabric Port Types	All ports are universal, auto-discovering, self-configuring and can assume the following states: ■ F_Port; supports N_Port ID Virtualization (NPIV) ■ FL_Port (public loop) ■ E_Port (switch-to-switch) ■ G_Port (generic) ■ GL_Port (generic loop)
Port Security	Port binding through a list of up to 32 WWPNs that are permitted to access the port.
Port Statistics	■ Configuration and operational data ■ Transmitted and received frame counts ■ Transmitted and received error counts

Table A-4. Modular Scalability (Continued)

Media Type (ordered separately)	
■ 8-Gbps I/O blade	Hot-pluggable, industry standard 3.3 volt SFP+ transceivers (for 8 Gbps speed) or SFP transceivers (for 4 and 2 Gbps speed)
■ 4-Gbps I/O blade	Hot-pluggable, industry standard 3.3 volt SFPs for 4/2/1 Gbps speeds
■ 10-Gbps I/O blade	Hot-pluggable, indusatry-standard X2 optical transceivers or X2 copper ISL cables for 10 Gbps speed
SFP Transceiver Types	■ Short Wave (optical) ■ Long Wave (optical) ■ Active/Passive Copper (8/4/2-Gbps)
X2 Transceiver Types	■ Short Wave (optical) ■ Long Wave (optical)
Transmission Ranges	Optical Media @ 10-Gbps ■ Short Wave: 300 m (984 ft.) ■ Long Wave: 5.18 km (8.34 miles)
Optical Cable Types (4-Gbps, 10-Gbps)	■ 50/62.5 micron multimode fiber optic ■ 9 micron single-mode fiber optic

Interoperability/Certifications

Table A-5. Interoperability/Certifications

Interoperability................................	Fully interoperable with all QLogic SANpro switch products ■ Compatible with FC-SW-2 compliant switches, including Brocade®, Cisco® and McDATA®. ■ Management interoperability with leading SAN management applications ■ SNIA SMI-S compliant ■ Certified with leading SAN hardware and software vendors. Visit http://www.qlogic.com/interoperability/interoperability.aspx for a comprehensive listing
SANmark™	SCD-3001v2a1 (E_Port) SCD-3002v2 (FL_Port) SCD-3010v1 (RSCN) SCD-3020v1 (Zoning)

Fabric Services

Table A-6. Fabric Services

Software Releases	■ QuickTools verion 7.08.03 ■ Enterprise Fabric Suite 2007 version 7.08.03 ■ Firmware version 7.8.03 or later
Ethernet Connections	
CPU Blade....................................	RJ-45 Ethernet connector on each CPU blade on back of chassis
Maintenance Panel.........................	Two alternate RJ-45 Ethernet connectors on front of chassis
IPv6 support	

Table A-6. Fabric Services (Continued)

Management Methods....................	■ Enterprise Fabric Suite 2007 Graphical User Interface (GUI) ■ QuickTools Web Applet ■ Application Programming Interface ■ Command Line Interface (CLI) ■ GS-4 Management Server ■ Simple Network Management Protocol (SNMP) ■ Remove Authentication Dial-In User Service (RADIUS) ■ File Transfer Protocol (FTP) ■ Trivial File Transfer Protocol (TFTP) ■ Storage Management Initiative (SMI-S)
Fabric Security	■ Fabric binding through a list of domain IDs and Switch WWNs ■ Secure Shell (SSH) for CLI ■ Secure Socket Layer (SSL) for QuickTools, ■ Enterprise Fabric Suite 2007 and SMI-S. ■ Local security database configuration ■ Remote authentication via a RADIUS Server ■ Additional MS request authentication through FCGS4 ■ CT authentication ■ Enable/Disable in-band management of switch
Registered State Change .... Notification (RSCN)	■ RSCNs are generated per standard (FC-GS, FCFS, FC-SW) ■ Delayed to allow consolidation into single RSCN ■ QLogic I/O StreamGuard™ suppresses RSCNs between initiators
Fabric Diagnostics..........................	Optional SANdoctor software package

Maintainability

Table A-7. Maintainability

Maintenance Strategy....................	Customer Replaceable Units (CRU) ■ SFP and X2 transceivers ■ I/O blades (8 maximum) ■ CPU blades (2) ■ Power supply blades (2) ■ Fan blades (2)
Data Integrity	Enhanced data integrity on all data paths
Fabric Shortest Path First (FSPF) ..	FSPF rerouting around failed links
SNMP Integration	Integration with SNMP managers
Firmware	Non-disruptive firmware code load and activation (NDCLA)
Switch Configurations....................	Easy configuration, save, and restore
Maintenance Access Methods	■ Single point in-band management with auto discovery across multiple switches ■ One out-of-band Ethernet 10/100Mb Base T RJ-45 management port per CPU Blade, each replicated on Maintenance Panel ■ One RJ-45 serial port per CPU Blade (RJ-45 to DB-9 conversion dongle included) ■ FC-GS4 Management Server
Power-On Self Test Diagnostics.....	Power-On Self Test (POST) tests all functional components except transceivers.
SANdoctor Diagnostics .... (optional)	■ FC Ping: verifies functional path existence between two ports ■ FC Trace route: displays path information between a source and destination ■ Digital Diagnostics Monitoring: displays real-time SFP, X2, and XPAK transceiver data

Table A-7. Maintainability (Continued)

Visual User Interface	LED indicators on the Maintenance Panel, I/O blades, CPU blades, Power Supply blades, Fan blades
Maintenance Panel.........................	Dual redundant Maintenance Panel EPROMs maintain chassis-specific information (such as WWN, SNMP System Object ID, Serial Number, Part Number, etc.), alternate Ethernet management interface ports, and LED summary status information for the switch
Global Services	Standard 1 year hardware/firmware warranty. SAN Pro Service and Support Programs: ■ SAN Pro Preferred standard: Next Business Day (NBD) Advanced Delivery spares, 24x7 technical phone support ■ Optional: upgrades to SAN Pro Choice (NBD Onsite Replacement) and SAN Pro Prime (4-hour Onsite Replacement) available for a fee

Physical Characteristics

Table A-8. Physical Characteristics

Enclosure/Blade Packaging	
■ Standard Chassis.......................	Includes Mounting Rail kit and two power cords
■ I/O Blades	Standard and optional I/O blades do not include SFPs, X2 transceivers, or copper/optical cables (orderable separately)
■ Hardware and Software .... License Field Upgradeability:	■ Model 9100 to model 9200 ugrade ■ Model 9200 to Fault Tolerant Model 9200 ■ One Model 9200 to HyperStack model ■ Two Model 9200 to HyperStack model

Table A-8. Physical Characteristics (Continued)

Dimensions	
■ Width..	431 mm (17.0”) 19 inch rack mount
■ Height.......................................	179 mm (7.0”) (4U)
■ Depth	673 mm (26.5”)
Weight .... (Model 9200, 8 I/O blades)	40.82 Kg (90 lbs)
Power Supply/Cooling	Hot-pluggable/dual-redundant Power Supply blades with integrated cooling fans ■ Dual 7'6" long 3-wire 16AWG power cables with IEC320 input connector ■ Hot-pluggable/dual-redundant fans ■ Back-to-Front Airflow Pattern Standard ■ 150 CFM air flow ■ 1,000 Watts (3,414 BTU/hour) per power supply
Heat Output .... Model 9200 with eight I/O blades including SFPs.	2,046 BTU/hour at 128-ports 4-Gb Fibre Channel (local switching) 4,228 BTU/hour at 256-ports 4-Gb Fibre Channel HyperStack (local switching)

Electrical Requirements

Table A-9. Electrical Requirements

Operating Voltage/Frequency.........	100 to 240 VAC auto-sensing, single phase; 47 to 63 Hz
Power Source Loading .... (maximum power supply rating)	10 Amps at 100 VAC 4.2 Amps at 240 VAC
Operating Load............................... Model 9200 with two I/O blades including SFPs	No data traffic: ■ 550 Watts at 128-ports 4-Gbps ■ 1,120 Watts at 256-ports 4-Gbps Full data traffic: ■ 600 Watts at 128-ports 4-Gbps (local switching) ■ 1,240 Watts at 256-ports 4-Gbps HyperStack (local switching)
CRU Power Usage	
■ I/O blade w/16 4-Gbps SFPs	34 watts
■ I/O blade w/4 10-Gbps X2.......... copper cables	32 watts
■ I/O blade w/4 10-Gbps X2.......... optical transcievers	35 watts
■ CPU blade.................................	80 watts
■ Fan blade	45 watts
Circuit Protection	Internally fused

Power Cord Specifications

The switch comes with two power cords with NEMA 5-15 non-locking plugs (SKU: CPK-9000-US). This power cord is approved for North America (USA, Canada, Puerto Rico), Mexico, Central America, South America, Korea, Taiwan, Phillippines, and Thailand. A similar power cord with a locking plug is also available ((SKU: CPK-9000-USL). QLogic offers power cords for additional regions/countries as listed in Table A-10.

Table A-10. Availalbe Power Cords

Region/Country	Specification	QLogic SKU Number
Argentina	IRAM 2073.1982 Plug	CPK-9000-AR
Australia	AS/NZS 3112 Plug	CPK-9000-AUNZ
Bahrain	BS1363/A Plug	CPK-9000-UKHK
China (PRC)	GB2099/GB1002-1 Plug	CPK-9000-CN
Denmark	Data DK-2-5A Plug	CPK-9000-DK
Europe	CEE 7/7 Plug	CPK-9000-CEE
Finland	CEE 7/7 Plug	CPK-9000-CEE
Greece	CEE 7/7 Plug	CPK-9000-CEE
Hong Kong/Macau (PRC)	BS1363/A Plug	CPK-9000-UKHK
Hungary	BS1363/A Plug	CPK-9000-UKHK
India	BS 546 Plug	CPK-9000-ZAIN
Indonesia	CEE 7/7 Plug	CPK-9000-CEE
International (special)	IEC 60309 Plug	CPK-9000-IEC
Ireland (Northern)	AS/NZS 3112 Plug	CPK-9000-AUNZ
Ireland (Southern)	BS1363/A Plug	CPK-9000-UKHK
Israel	SI-32 Plug	CPK-9000-IL
Italy	CEI 23-16/VII Plug	CPK-9000-IT
Japan	JIS 8303 PSE Plug	CPK-9000-JP
Malaysia	BS1363/A Plug	CPK-9000-UKHK
Middle East	CEE 7/7 Plug	CPK-9000-CEE
New Zealand	AS/NZS 3112 Plug	CPK-9000-AUNZ

Table A-10. Availalbe Power Cords (Continued)

Region/Country	Specification	QLogic SKU Number
Norway	CEE 7/7 Plug	CPK-9000-CEE
Russia	CEE 7/7 Plug	CPK-9000-CEE
Singapore/Brunei	BS1363/A Plug	CPK-9000-UKHK
South Africa	BS 546 Plug	CPK-9000-ZAIN
Sweden	CEE 7/7 Plug	CPK-9000-CEE
Switzerland	SEV 1011 Plug	CPK-9000-CH
Tasmania	AS/NZS 3112 Plug	CPK-9000-AUNZ
United Kingdom	BS1363/A Plug	CPK-9000-UKHK

Environmental Factors

Table A-11. Environmental Factors

Temperature	
■ Operating	0 to 40°C (32 to 104°F)
■ Non-operating	- 40 to 70°C (-40 to 158°F)
Humidity	
■ Operating	15% to 80%, non-condensing
■ Non-operating	5% to 90%, non-condensing
Altitude	
■ Operating	0 to 3048m (0 to 10,000 feet)
■ Non-operating	0 to 15,240m (0 to 50,000 feet)
Vibration	IEC 68-2
■ Operating	5-500 Hz, random, 0.2 G rms, 10 minutes
■ Non-operating	5-500 Hz, random, 2.1 G rms, 10 minutes
Shock	IEC 68-2
■ Operating	4 g, 11ms, 20 repetitions
■ Non-operating	30g, 292 ips, 13 msec, trapezoidal pulse

Regulatory Certifications

Table A-12. Regulatory Certifications

Safety Standards	UL 60950 (USA) CSA 22.2 60950-1 (Canada) EN60950-1 (EC) CB Scheme-IEC 60950-1 (International) GOST R MEK 60950 (Russia)
Emissions Standards	FCC Part 15B Class A (USA) VCCI-3/2005 Class A ITE (Japan) ICES-003 Issue 4 Class A ITE (Canada) EN 55022 Level A (EC) BSMI CNS 13438 Class A (Taiwan) CISPR 22 Class A (international) AS/NZA CISPR 22:2002 Class A (AUS/NZ) GOST R (Russia) 12/KNxx (Korea)
Environmental Standards	RoHS-6/WEEE (EU and Japan)
Voltage Fluctuations	EN 61000-3-2, 3
Harmonics	EN 61000-3-2
Immunity	EN 55024:1998
Marking	FCC Part 15, UL (United States) cUL, CUE, TUV (Canada) TUV , CUE, CE (EC) VCCI-A (Japan) C-Tick (AUX/NZ) GOST R (Russia) MIC (Korea) Exempt (Taiwan) UL AR/S-Mark (Argentina)

Notes

Glossary

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

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

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

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.

ASIC

Application Specific Integrated Circuit

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Challenge-Handshake Authentication Protocol

An authentication protocol by which a device is challenged to verify its identity before being allowed to log in to a switch.

Chassis Hop

A measure of fabric latency represented by the ISL that any frame crosses when travelling from one switch to another. A frame that travels from one switch to another over an ISL experiences one chassis hop.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Common Information Model

Switch service that provides for switch management through third-party applications that comply with SMI-S.

Configuration Wizard

An Enterprise Fabric Suite 2007 or Quick-Tools wizard that automates the switch configuration process.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

CRU

Customer Replaceable Unit

Default Visibility

Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Domain ID

User defined number that identifies the switch in the fabric.

Enterprise Fabric Suite 2007

Workstation-based switch management application.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Extended Credits

A feature that enables you to reallocate port buffer credits to extend transmission distances.

Fabric Database

The set of fabrics that have been opened during a Enterprise Fabric Suite 2007 session.

Fabric Device Management Interface

An interface by which device host bus adapters can be managed through the fabric.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port or FL_Port.

Fabric Security

The functions that provide security for fabric users and devices including user account security and fabric services.

Fabric Services

A component of fabric security that provides for the control of inband management and SNMP on a switch.

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous Enterprise Fabric Suite 2007 session.

Fault Tolerant

A licensed feature that supports automatic and manual failover of switch management functions from the primary CPU blade to the secondary CPU blade.

FDMI

See Fabric Device Management Interface.

Flash Memory

Memory on the switch that contains the chassis control firmware.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

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 chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

HyperStack

A licensed feature that supports the connection of two QLogic 9000 Series switches through the multiple 10-Gbps link Inter-Chassis Connectors (ICC).

Inactive Firmware

The firmware image on the switch that is not in use.

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.

Inter-Switch Link

The connection between two switches using E_Ports.

I/O Blade

Fibre Channel component of the QLogic 9000 Series switch.

IP

Internet Protocol

License Key

A code associated with a separately-purchased feature that activates that feature on the switch.

LIP

Loop Initialization Primitive sequence

Maintenance Button

Momentary button on the switch used to place the switch in 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

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Merge Auto Save

Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

MIB

Management Information Base

Network Time Protocol

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

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

NTP

Network Time Protocol

Pending Firmware

The firmware image that will be activated upon the next switch reset.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

QuickTools

Switch management application that is resident in the switch firmware and executed through an internet browser.

Remote Authentication Dial-in Server

A server that supports the remote authentication of user and device logins to a switch.

SANdoctor

A licensed feature that provides for media diagnostics, Fibre Channel trace, and Fibre Channel ping functions.

Secure Shell

Protocol that secures connections to the switch for the command line interface.

Secure Socket Layer

Protocol that secures connections to the switch for Enterprise Fabric Suite 2007, QuickTools, the API, and SMI-S.

Security Set

A set of up to three groups that define device security for the switch.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SMI-S

Storage Management Initiative–Specification.

SNMP

Simple Network Management Protocol

Storage Management Initiative–Specification

A standard that provides for the management of the switch through third-party management applications.

Target

A storage device that responds to an initiator device.

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.

VCCI

Voluntary Control Council for Interference

Worldwide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

Worldwide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Notes

Index

Notes

QLOGIC®
The Ultimate in Performance

Corporate Headquarters QLogic Corporation 26650 Aliso Viejo Parkway Aliso Viejo, CA 92656 949.389.6000 **www.qlogic.com**

Europe Headquarters QLogic (UK) LTD. Quatro House Lyon Way, Frimley Camberley Surrey, GU16 7ER UK +44 (0) 1276 804 670