Sun Storage Fibre Channel Switch 5802 Installation Guide

Firmware Version 7.4

Sun Microsystems, Inc.
www.sun.com

Part No. 820-4969-10
September 2008, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

Figures

Tables

Preface

This guide describes the features and installation of the Sun Storage Fibre Channel Switch 5802. The Sun Storage Fibre Channel Switch 5802 is a 24-port, 8-Gbit/sec Fibre Channel switch. This guide 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.

How This Document Is Organized

This manual is organized as follows:

- Chapter 1 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Chapter 2 describes the factors to consider when planning a fabric.
- Chapter 3 explains how to install and configure the switch.
- Chapter 4 describes the diagnostic methods and troubleshooting procedures.
- Chapter 5 describes the removal and replacement of field replaceable units: media transceivers and power supplies.
- Appendix A lists the switch specifications.

Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`

`AaBbCc123`	What you type, when contrasted with on-screen computer output	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this. To delete a file, type `rm` *filename*.

Note – Characters display differently depending on browser settings. If characters do not display correctly, change the character encoding in your browser to Unicode UTF-8.

Related Documentation

The following table lists the documentation for this product. The online documentation is available at:

`http://docs.sun.com/app/docs/prod/switch.dir#hic`

Application	Title	Part Number	Format	Location
Regulatory and safety information	*Sun Storage Regulatory and Safety Compliance Manual*	820-5506-*xx*	PDF	Online
Hardware and software requirements	*Sun Storage Fibre Channel Switch 5802 Hardware Release Notes*	820-5539-*xx*	PDF	Online
Initial switch installation	*Sun Storage Fibre Channel Switch 5802 Setup*	820-4950-*xx*	Printed PDF	Shipping kit Online

Application	Title	Part Number	Format	Location
Manage the switch	*Sun Storage Fibre Channel Switch 5802 QuickTools User Guide*	820-4972-*xx*	PDF	Online
Manage the switch	*Enterprise Fabric Suite 2007 User Guide*	820-4966-*xx*	PDF	Enterprise Fabric 2007 CD Online
Manage the switch	*Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide*	820-4960-*xx*	PDF	Online
Command line interface reference	*Command Line Interface Quick Reference Guide*	820-4962-*xx*	PDF	Online
Look up messages and correct problems	*Event Message Guide*	820-4971-*xx*	PDF	Online
Manage the switch	*Simple Network Management Protocol Reference Guide*	820-4974-*xx*	PDF	Online
Manage the switch	*CIM Agent Reference Guide*	820-4959-*xx*	PDF	Online

Documentation, Support, and Training

Sun Function	URL
Documentation	`http://www.sun.com/documentation/`
Support	`http://www.sun.com/support/`
Training	`http://www.sun.com/training/`
Service	`http://www.sun.com/service/contacting/index.xml`

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

`http://www.sun.com/hwdocs/feedback`

Please include the title and part number of your document with your feedback:

Sun Storage Fibre Channel Switch 5802 Installation Guide, part number 820-4969-10.

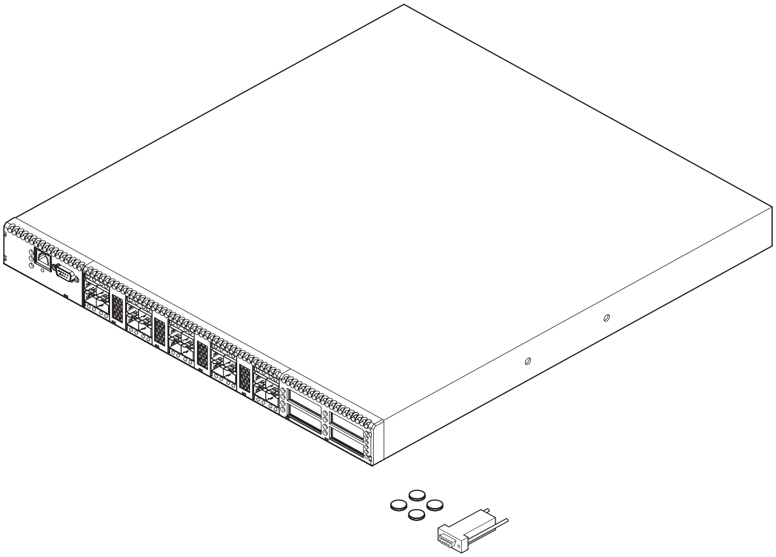
CHAPTER 1

General Description

The Sun Storage Fibre Channel Switch 5802, shown in FIGURE 1-1, is a 24-port 8-Gbit/sec Fibre Channel switch with both Ethernet and serial management interfaces. This chapter describes the features and capabilities of the Sun Storage Fibre Channel Switch 5802 and includes information about the following features:

- Chassis Controls and LEDs
- Fibre Channel Ports
- Ethernet Port
- Serial Port
- Power Supplies and Fans
- Switch Management

FIGURE 1-1 Sun Storage Fibre Channel Switch 5802



Fabrics are managed with the Command Line Interface (CLI), the QuickTools™ web applet for Sun FC switches and directors, or the Enterprise Fabric Suite™ 2007 application for Sun FC switches and directors.

- Refer to *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for more information about the CLI.
- Refer to the *Sun Storage Fibre Channel Switch 5802 QuickTools User Guide* for information about QuickTools.
- Refer to the *Enterprise Fabric Suite 2007 User Guide* for information about using the Enterprise Fabric Suite 2007 application.

Chassis Controls and LEDs

The chassis LEDs provide information about the switch's operational status. These LEDs include the Input Power LED (green), Status (OK) LED (green), and the System Fault LED (amber) as shown in FIGURE 1-2. The Maintenance button shown in FIGURE 1-2 is the only chassis control and is used to reset a switch or to recover a disabled switch. To apply power to the switch, plug the power cords into the switch AC power receptacles, located on the back of the switch, and into a 100–240 VAC power source.

FIGURE 1-2 Chassis LEDs and Controls

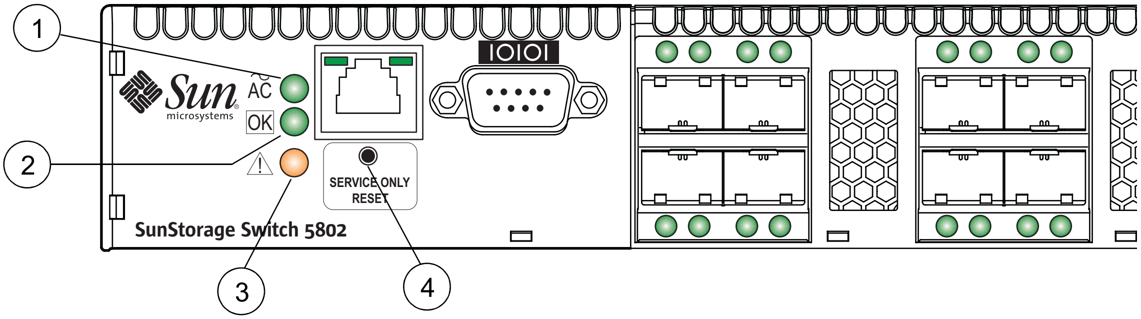


Figure Legend

1	Input Power LED (Green)
2	Status (OK) LED (Green)
3	System Fault LED (Amber)
4	Maintenance Button

Input Power LED (Green)

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

Status (OK) LED (Green)

The Status (OK) LED indicates the status of the internal switch processor and the results of the POST. Following a normal power-up, the Status (OK) LED illuminates continuously. In maintenance mode, the Status (OK) LED will flash.

System Fault LED (Amber)

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. Fault conditions include POST errors, over-temperature conditions, and power supply malfunctions.

Maintenance Button

The Maintenance button, shown in FIGURE 1-2, is a dual-function momentary switch on the front panel. Its purpose is to reset the switch or to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to "Recovering a Switch Using Maintenance Mode" on page 69 for more information.

Resetting a Switch

To reset the switch, press and hold the Maintenance button for less than 2 seconds. The switch will respond as follows:

1. All the chassis LEDs will illuminate except the System Fault LED.
2. After approximately 1 minute, the power-on self test (POST) begins, extinguishing the Status (OK) LED.
3. When the POST is complete, the Input Power LED is illuminated and the Status (OK) LED is continuously illuminated.

Placing the Switch in Maintenance Mode

To place the switch in maintenance mode, do the following:

1. **Isolate the switch from the fabric.**
2. **Press and hold the Maintenance button with a pointed tool for a few seconds until the Status (OK) LED extinguishes, then release the button. The Status (OK) LED flashes while the switch is in maintenance mode.**

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

Fibre Channel Ports

The Sun Storage Fibre Channel Switch 5802 has 20 Fibre Channel Small Form-Factor Pluggable (SFP) ports and four Fibre Channel XPAK ports. SFP ports are numbered 0–19 as shown in FIGURE 1-3. Each SFP port is served by an SFP optical transceiver and is capable of 1-, 2-, 4-, or 8-Gbit/sec transmission. SFP ports are hot-pluggable and can self-discover both the port type and transmission speed when connected to devices or other switches. The port LEDs are located above ports 0–9 and below ports 10–19, and provide port login and activity status information.

The XPAK ports are numbered 20–23 as shown in FIGURE 1-3. Each XPAK port is served by an XPAK optical transceiver or an XPAK switch stacking cable. An XPAK port is capable of 12.75-Gbit/sec transmission or 25.5-Gbit/sec with the optional license key. XPAK ports are hot-pluggable and can self-discover transmission speed when connected to devices or other switches. The XPAK switch stacking cable is a passive cable and transceiver assembly for connecting to other XPAK-capable switches. The XPAK ports come with covers that must be removed before installing transceivers or cables. XPAK port LEDs are located to the left of their respective ports and provide port login and activity status.

FIGURE 1-3 Fibre Channel Ports

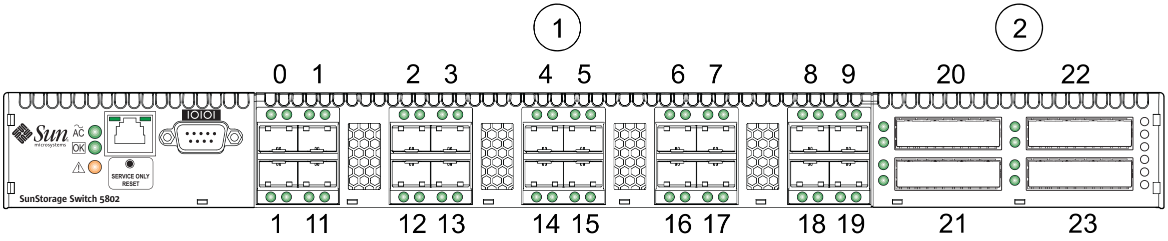


Figure Legend

1	SFP Ports
2	XPAK Ports

Each SFP port is capable of 1-, 2-, 4-, or 8-Gbit/sec transmission depending on the SFP. SFP ports are hot-pluggable and can self-discover both the port type and transmission speed when connected to devices or other switches. The SFP port LEDs are located above their respective ports and provide port login and activity status information.

Note – Setting an SFP port to 1-Gbit/sec that has an 8-Gbit/sec SFP transceiver will down the port.

The Sun Storage Fibre Channel Switch 5802 can be a 12-, 16-, 20-, or 24-port switch. This means that the four XPAK ports 20–23 are enabled plus varying numbers of SFP ports. For example, the base 12-port switch enables the four XPAK ports and SFP ports 0–7. License keys are available from your authorized reseller to enable additional SFP ports or upgrade the XPAK ports to 20-Gbit/sec. Refer to "Feature Licensing" on page 19 for more information.

You can choose which ports are active using Enterprise Fabric Suite 2007.

Port LEDs

Each port has its own Logged-In LED (L) and Activity LED (A) as shown in FIGURE 1-4.

FIGURE 1-4 Port LEDs

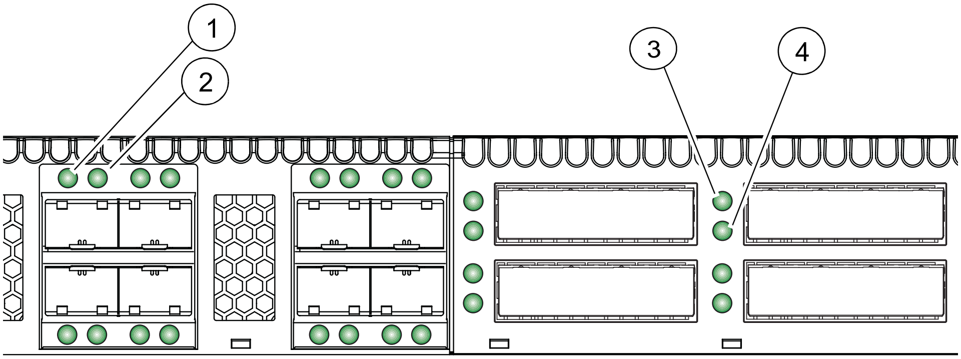


Figure Legend

1	SFP Port Logged-In LED
2	SFP Port Activity LED
3	XPAK Port Logged-In LED
4	XPAK Port Activity LED

Port Logged-In LED (Green)

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-In LEDs. Following a successful port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-In LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-In LED is extinguished. Refer to "Logged-In LED Indications" on page 64 for more information about the Logged-In LED.

Port Activity LED (Green)

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

Transceivers

The Sun Storage Fibre Channel Switch 5802 supports SFP optical transceivers for the SFP ports and XPAK optical transceivers or XPAK stacking cables for the XPAK ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fiber optic cables plug into the SFP transceivers which then connect to the devices. An SFP port is capable of transmitting at 1-, 2-, 4-, or 8-Gbit/sec; however, the transceiver must also be capable of delivering at these rates.

The SFP and XPAK 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 "Install Transceivers" on page 49 for information about installing and removing SFP and XPAK optical transceivers.

Port Types

the Sun Storage Fibre Channel Switch 5802 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 SFP ports configured as GL_Ports. The XPAK ports come from the factory configured as G_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a loop device, as an F_Port when connected to a single device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- A G_Port self-configures as an F_Port when connected to a single device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single device (N_Port).
- An F_Port supports a single device.
- E_Ports enable you to expand the fabric by connecting switches together.

The Sun Storage Fibre Channel Switch 5802 self-discovers all inter-switch connections. Refer to "Multiple Chassis Fabrics" on page 20 for more information.

Ethernet 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 as shown in FIGURE 1-5. A management workstation can be a Windows, Solaris™ Operating System (OS), or a Linux workstation that is used to configure and manage the switch fabric. You can manage the switch over an Ethernet connection using the CLI, QuickTools, or SNMP.

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

FIGURE 1-5 Ethernet Port

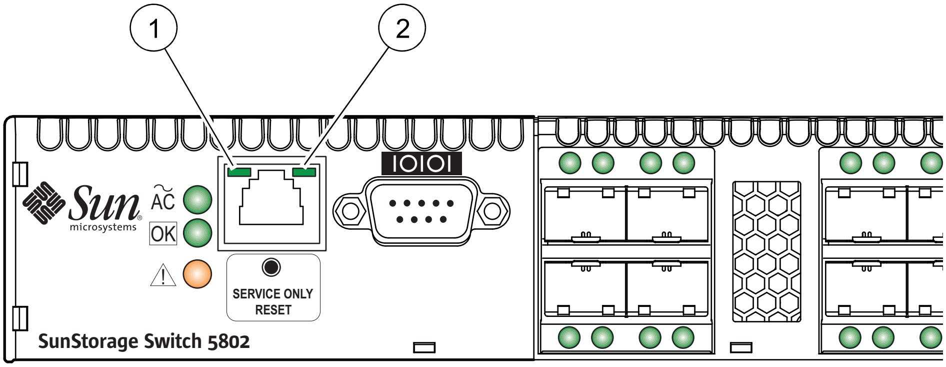


Figure Legend Sun Storage Fibre Channel Switch 5802

1	Activity LED
2	Link Status LED

Serial Port

The Sun Storage Fibre Channel Switch 5802 is equipped with an RS-232 serial port for maintenance purposes as shown in FIGURE 1-6. You can manage the switch through the serial port using the CLI.

FIGURE 1-6 Serial Port and Pin Identification

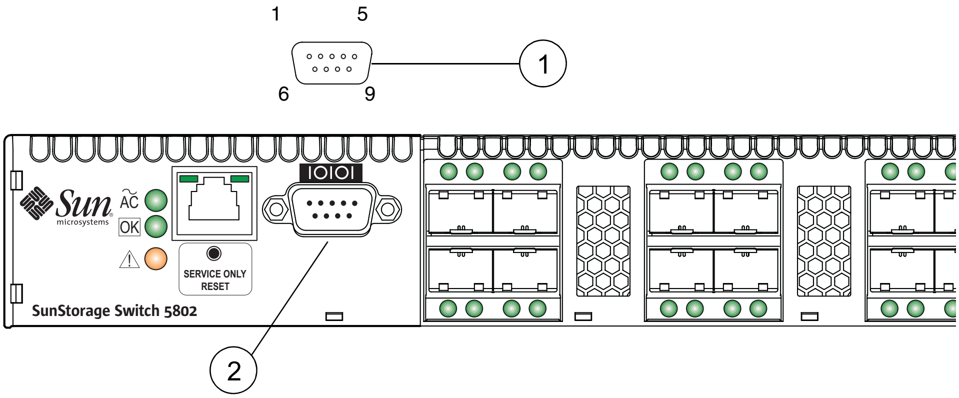


Figure Legend

1	RS-232 Connector Pin Identification
2	Serial Port

The switch comes with a DB9-to-RJ-45 adapter with which you can connect the workstation to the switch with a 10/100 Base-T Ethernet straight cable. The pins on the switch RS-232 connector are shown in FIGURE 1-6 and identified in TABLE 1-1. Refer to "Connect the Workstation to the Switch" on page 53 for information about connecting the management workstation through the serial port.

TABLE 1-1 Serial Port Pin Identification

Pin Number	Description
1	Carrier Detect (DCD)
2	Receive Data (RxD)
3	Transmit Data (TxD)
4	Data Terminal Ready (DTR)
5	Signal Ground (GND)
6	Data Set Ready (DSR)

TABLE 1-1 Serial Port Pin Identification

Pin Number	Description
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

Power Supplies and Fans

The Sun Storage Fibre Channel Switch 5802 has two, hot pluggable power supplies that convert standard 100–240 VAC to DC voltages for the various switch circuits. Each power supply has an AC power receptacle and two status LEDs as shown in FIGURE 1-7:

- The Power Supply Status LED (green) illuminates to indicate that the power supply is receiving AC voltage and producing the proper DC voltages.
- The Power Supply Fault LED (amber) illuminates to indicate that a power supply fault exists and requires attention.

FIGURE 1-7 Power Supplies

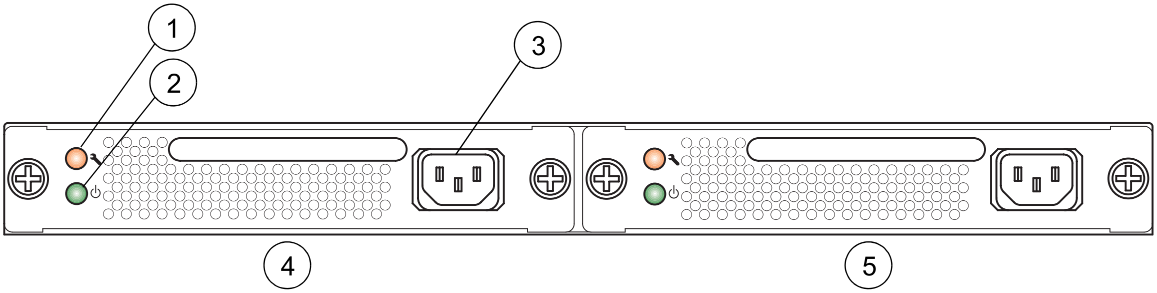


Figure Legend

1	Fault LED (Amber)
2	Status LED (Green)
3	AC Power Receptacle
4	Power Supply 1
5	Power Supply 2

Each power supply is capable of providing all of the switch's power needs. During normal operation, each power supply provides half of the demand. If one power supply goes offline, the second power supply steps up and provides the difference.

The power supplies are hot swappable and interchangeable. Hot pluggable means that you can remove and replace one power supply while the switch is in operation without disrupting service. Refer to Chapter 5 for information about replacing the power supplies.

Connecting a power supply to an AC voltage source energizes the switch logic circuitry. Internal fans provide cooling. Air flow is front-to-back.

Switch Management

The switch supports the following management tools:

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

QuickTools Web Applet

To provide basic switch management tools in a graphical user interface and to make switch management less dependent on a particular platform, each switch contains a web applet called QuickTools. QuickTools is designed to provide switch management for fabrics with less than four switches. For larger fabrics, consider the optional management application, Enterprise Fabric Suite 2007.

You run QuickTools by opening the switch IP address with an internet browser. QuickTools provides the following management features:

- Faceplate device management
- Switch and port statistics
- Configuration wizard
- Zoning administration
- Fabric tree for fabric management

- User account configuration
- Switch and fabric events
- Operational and environmental statistics
- Global device nicknames
- Online help

For more information, refer to the *Sun Storage Fibre Channel Switch 5802 QuickTools User Guide*.

Enterprise Fabric Suite 2007

Enterprise Fabric Suite 2007 is an optional workstation-based Java™ application that provides a graphical user interface for full fabric and switch management. Enterprise Fabric Suite 2007 is designed for managing fabrics of four or more switches and can be installed on an unlimited number of workstations. Enterprise Fabric Suite 2007 can run on a Windows, Solaris OS, or Linux workstation. Enterprise Fabric Suite 2007 provides all of the management features of QuickTools plus the following:

- Fabric tracker for monitoring fabric firmware versions
- Port threshold alarm configuration
- Topology display for fabric management
- Stack management
- Performance View for port performance
- Extended Credits Wizard
- Zoning Wizard
- Moveable active ports

To purchase Enterprise Fabric Suite 2007, contact your authorized reseller. Refer to the *Enterprise Fabric Suite 2007 User Guide* for information about the Enterprise Fabric Suite 2007 application and its use.

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 *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for more information.

Application Programming Interface

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

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. Sun Storage 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. Refer to the *Simple Network Management Protocol Reference Guide* for more information.

You must use the CLI to configure SNMP version 3. Refer to the Snmpv3user command in the *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide*.

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

FTP and TFTP provide the command line interface for exchanging files between the switch and the management workstation. These files include firmware image files, configuration files, and log files.

CHAPTER 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 number of devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches.

Consider the transmission speeds of your HBAs and SFPs. The switch ports 0–19 support 1-Gbit/sec, 2-Gbit/sec, 4-Gbit/sec, and 8-Gbit/sec transmission speeds depending on the SFP.

Note – Setting an SFP port to 1-Gbit/sec that has an 8-Gbit/sec SFP transceiver will down the port.

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

Device Access

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

- 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).
MaxAliases	Maximum number of aliases (2500).
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (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 Sun Storage Fibre Channel Switch 5802 supports class 2 and class 3 Fibre Channel service at transmission rates of 1-, 2-, 4-, 8-, 10-, or 20-Gbit/sec with a maximum frame size of 2148 bytes. Each Fibre Channel 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 SFP 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 Fibre Channel SFP port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fiber optic cables, this enables full bandwidth over the following approximate distances:

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

With Enterprise Fabric Suite 2007, longer distances can be spanned at full bandwidth on SFP ports by extending credits to G_Ports, F_Ports, and E_Ports. Each port can donate 15 credits to a pool from which a recipient port can borrow. However, SFP ports can borrow only from other SFP ports. XPAK ports cannot borrow or donate credits. The recipient port also loses a credit in the process. For example, you can configure an SFP recipient port to borrow 15 credits from one donor port for a total of 30 credits (15+15=30).

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 cause excessive port resets. TABLE 2-2 describes the possible distances and minimum cable lengths for a port with 30 credits.

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)	0.75 Km
8-Gbps	6 Km (30÷4.8)	0.37 Km

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-Gbit/sec 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. XPAK ports transmit at a nominal rate of 10-Gbit/sec which corresponds to a full duplex bandwidth value of 2550 MB. With a 20-Gbit/sec license key, XPAK ports can transmit at a nominal rate of 20-Gbit/sec (5100 MB bandwidth).

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-Gbit/sec source ports can transmit to one 4-Gbit/sec destination port. Similarly, one source port can feed multiple destination ports if the combined destination bandwidth is greater than or equal to the source bandwidth.

In multiple chassis fabrics, each link between chassis contributes 424, 850, 1700, 2550, or 5100 megabytes of bandwidth between those chassis, depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order delivery with any number of links between chassis.

Latency

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

TABLE 2-3 Port-to-Port Latency

	Destination Rate					
	Gbps	**2**	**4**	**8**	**10**	**20**
Source Rate	2	< 0.6 µsec	< 0.7 µsec[1]	< 0.6 µsec[1]	< 0.6 µsec[1]	< 0.6 µsec[1]
	4	< 0.4 µsec	< 0.3 µsec	< 0.4 µsec[1]	< 0.4 µsec[1]	< 0.3 µsec[1]
	8	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec[1]	< 0.2 µsec[1]
	10	< 0.3 µsec	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec[1]
	20	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec

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

Feature Licensing

Note – License keys enable menu selections in Enterprise Fabric Suite 2007 and commands and keywords in the CLI. License keys do not affect the capabilities of the QuickTools web applet.

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 arrange to purchase license keys from your switch distributor or authorized reseller.

- The SANdoctor™ license key for Sun FC switches and directors 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).
- The Port Activation license key activates additional SFP ports for a total of 16, 20, or 24 ports.
- The 20-Gbit/sec license key enables the XPAK ports to transmit and receive at 25.5-Gbit/sec instead of the default 12.75-Gbit/sec.

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 60 for information about installing a license key.

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 switches together in a wide variety of topologies.

You can connect up to six switches together through the XPAK ports, thus preserving the SFP ports for devices. This is called stacking. The Sun Storage Fibre Channel Switch 5802 switch divides the XPAK port buffer to balance traffic across the connection. The XPAK ports operate with any standard XPAK interface. You can also connect the Sun Storage Fibre Channel Switch 5802 to other switches through the SFP ports in a wide variety of topologies. Consider your topology and cabling requirements.

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 Sun Storage Fibre Channel Switch 5802 provides the lowest latency of any product in its class. Refer to "Performance" on page 17 for information about latency. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance, place devices on the same switch under the following conditions:

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

Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple 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 *Sun Storage Fibre Channel Switch 5802 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. Domain ID reassignment has no effect on zone members defined by WWN.

Stacking

You can connect up to six switches together through the XPAK ports, thus preserving the SFP ports for devices. This is called stacking. The following 2-, 3-, 4-, 5-, and 6-switch stacking configurations are recommended for best performance and redundancy. Each XPAK port contributes 1.275 GB of bandwidth between chassis in each direction. This is equivalent to three SFP connections operating at 4-Gbit/sec. If you upgrade the XPAK ports to 20-Gbit/sec, this is equivalent to three SFP connections operating at 8-Gbit/sec. FIGURE 2-1 shows a two-switch stack of switches using two 3-inch XPAK switch stacking cables. Forty SFP ports are available for devices.

FIGURE 2-1 Two-Switch Stack

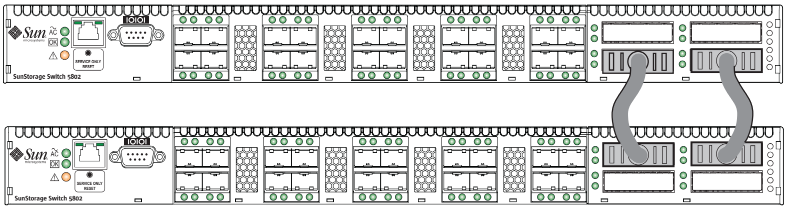


FIGURE 2-2 shows a three-switch stack of switches using two 3-inch and one 9-inch XPAK switch stacking cables. Sixty SFP ports are available for devices.

FIGURE 2-2 Three-Switch Stack

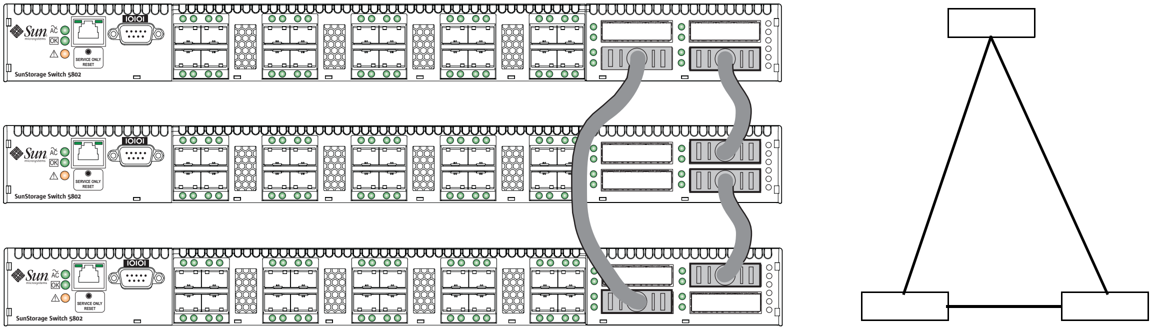


FIGURE 2-3 shows a four-switch stack of switches using three 3-inch and three 9-inch XPAK switch stacking cables. Eighty SFP ports are available for devices.

FIGURE 2-3 Four-Switch Stack

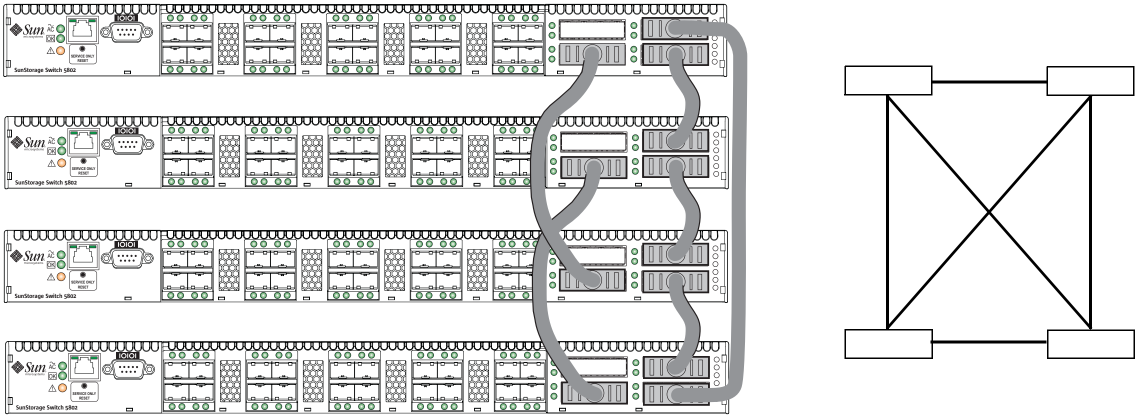


FIGURE 2-4 shows a five-switch stack of switches using ten XPAK switch stacking cables. One hundred SFP ports are available for devices.

FIGURE 2-4 Five Switch Stack

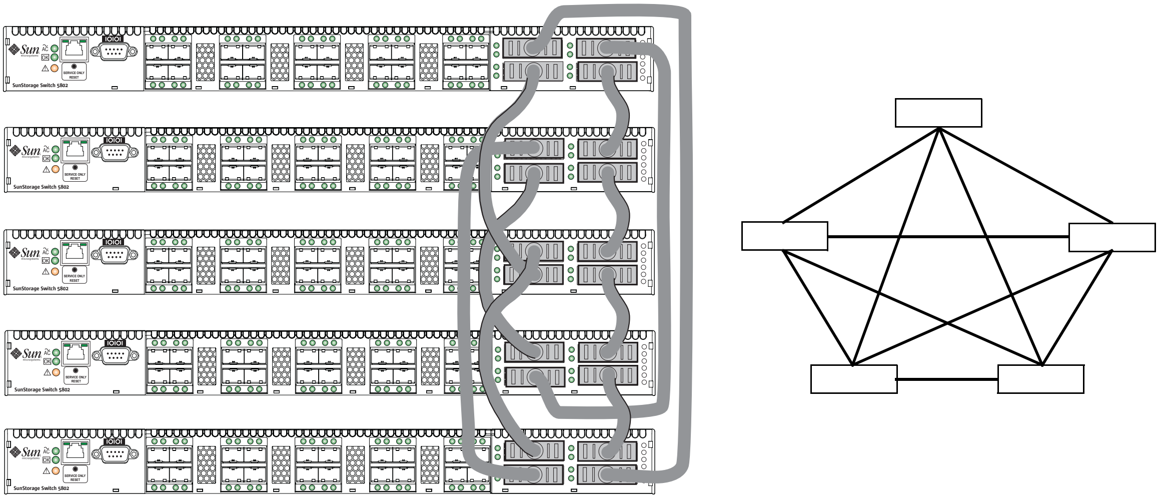
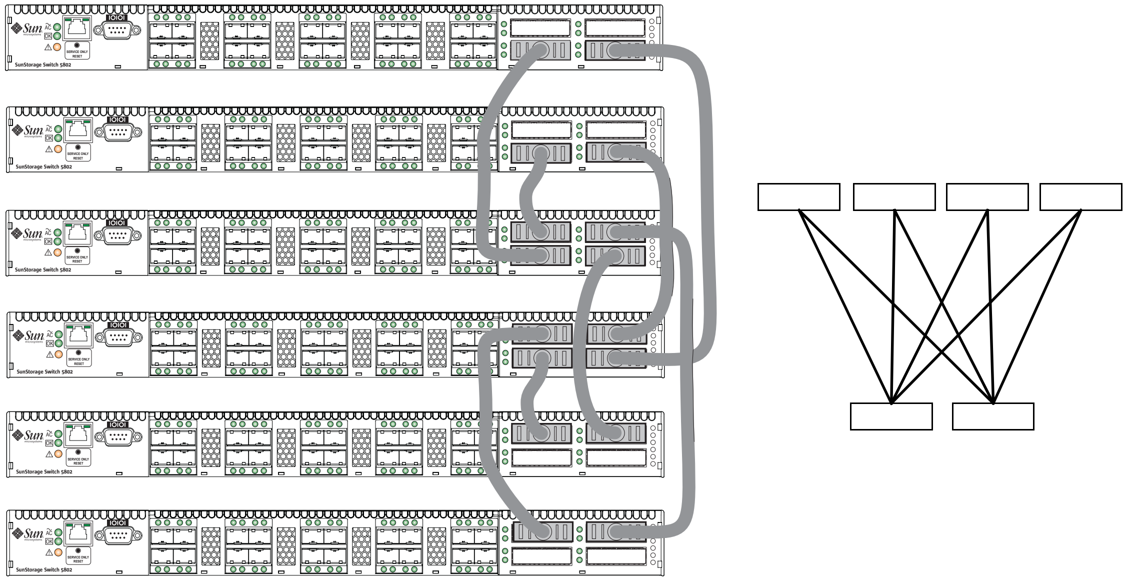


FIGURE 2-5 shows a stack of six switches using eight XPAK switch stacking cables. One hundred twenty SFP ports are available for devices.

FIGURE 2-5 Six Switch Stack



Common Topologies

Although the XPAK stacking ports achieve the highest cabling efficiency and bandwidth, you can also create multiple switch configurations using the SFP ports. The Sun Storage Fibre Channel Switch 5802 supports the following topologies using the SFP ports:

- Cascade Topology
- Mesh Topology
- MultiStage Topology

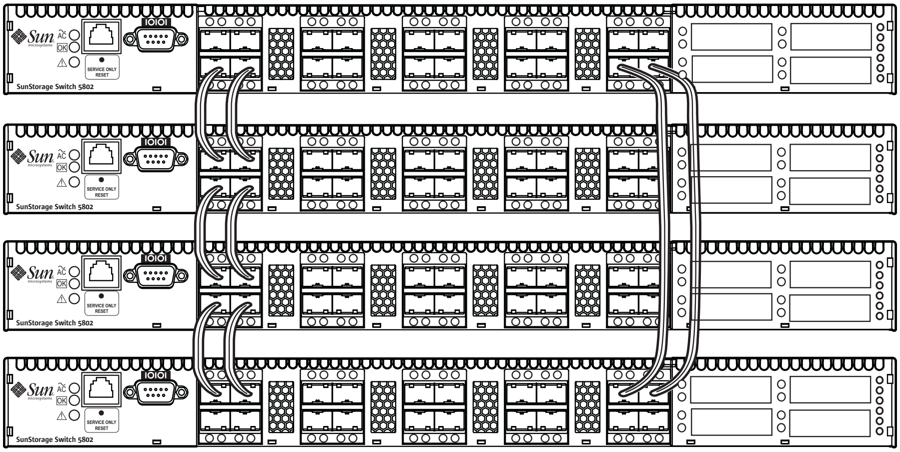
Cascade Topology

A cascade topology describes a fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology as shown in FIGURE 2-6. The loop reduces latency because any switch can route traffic in the shortest direction to any switch in the loop. The loop also provides failover should a switch fail.

Using 24-port Sun Storage Fibre Channel Switch 5802 switches, the cascade fabric shown in FIGURE 2-6 has the following characteristics:

- Each chassis link contributes up to 850 MB of bandwidth between chassis, 1700 MB in full duplex. However, because of the sequential structure, that bandwidth will be shared by traffic between devices on other chassis.
- Latency between any two ports is no more than two chassis hops.
- Sixty-four Fibre Channel SFP ports are available for devices.

FIGURE 2-6 Cascade-with-a-Loop Topology

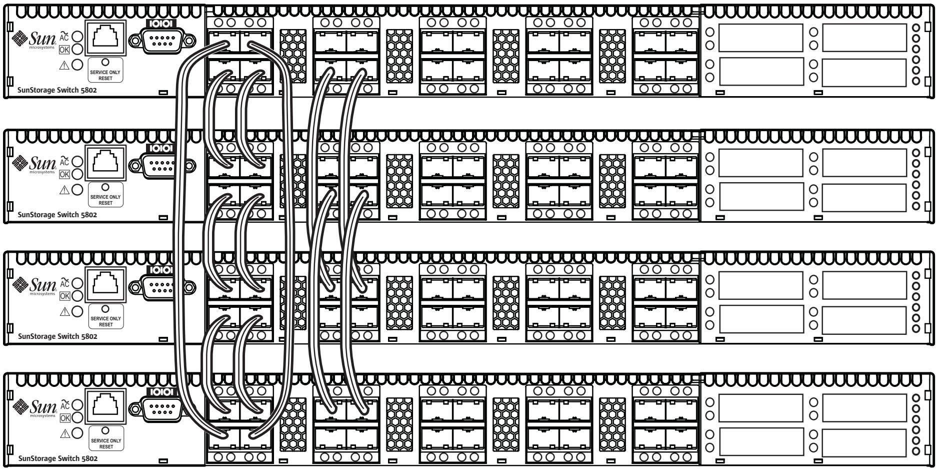


Mesh Topology

A mesh topology describes a fabric in which each chassis has at least one port directly connected to each other chassis in the fabric. Using 24-port Sun Storage Fibre Channel Switch 5802 switches the mesh fabric shown in FIGURE 2-7 has the following characteristics:

- Each link contributes up to 850 MB of bandwidth between switches, 1700 MB in full duplex. Because of multiple parallel paths, there is less competition for this bandwidth than with a cascade or a Multistage topology.
- Latency between any two ports is one chassis hop.
- Fifty-six Fibre Channel SFP ports are available for devices.

FIGURE 2-7 Mesh Topology



MultiStage Topology

A Multistage™ topology describes a fabric in which two or more edge switches connect to one or more core switches. Using 24-port Sun Storage Fibre Channel Switch 5802 switches, the Multistage fabric shown in FIGURE 2-8 has the following characteristics:

- Each link contributes up to 850 MB of bandwidth between chassis. Competition for this bandwidth is less than that of a cascade topology, but greater than that of the mesh topology.
- Latency between any two ports is no more than two chassis hops.
- Seventy-two Fibre Channel SFP ports are available for devices.

FIGURE 2-8 Multistage Topology

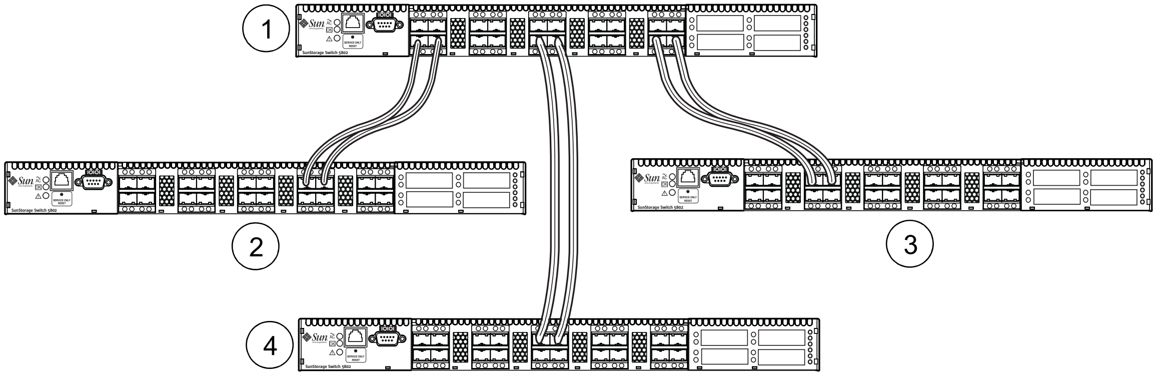


Figure Legend

1	Core Switch
2	Edge Switch
3	Edge Switch
4	Edge Switch

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 enabled.
- **QuickTools web applet (Embedded GUI)**: 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)**: Enables or disables the management of the switch through third-party applications that use GS-3 Management Server. The default is disabled.

- **Call Home:** Provides for automated e-mail 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 mail 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.

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
- IP Security
- Port Binding
- Connection Security
- 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. 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 31 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 31.

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 *Sun Storage Fibre Channel Switch 5802 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 CLI command. Refer to the *Sun Storage Fibre Channel Switch 5802 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).

- 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 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 "Internet Protocol Support" on page 29. A secure connection is required to authenticate user logins with a RADIUS server. Refer to "Connection Security" on page 31 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 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 2-9. 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 2-9 Security Example: Switches and HBAs

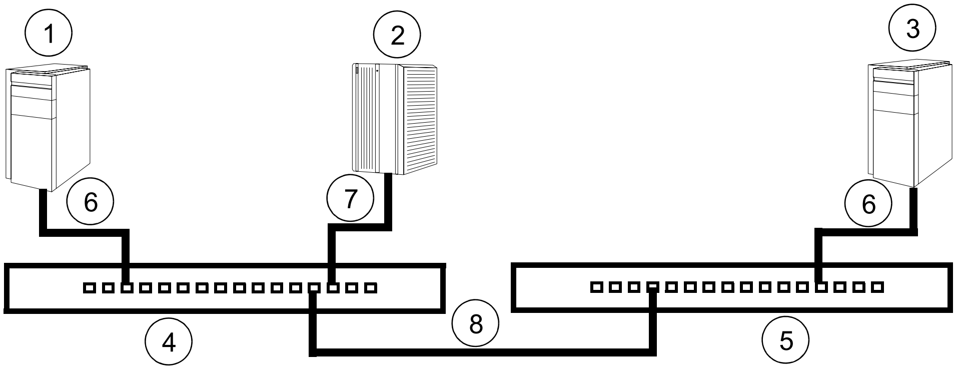


Figure Legend

1	**Device**: HBA_1 **WWN**: 10:00:00:c0:dd:07:c3:4d **Security**: Yes	**5**	**Device**: Switch_2 **WWN**: 10:00:00:c0:dd:07:e3:4e **Security**: Yes
2	**Device**: JBOD **WWNS:**10:00:00:d1:ee:18:d4:5e 10:00:00:d1:ee:18:d4:5f 10:00:00:d1:ee:18:d4:5g **Security:** No	**6**	F_Port
3	**Device**: HBA_2 **WWN**: 10:00:00:c0:dd:07:c3:4f **Security**: No	**7**	FL_Port
4	**Device**: Switch_1 **WWN**: 10:00:00:c0:dd:07:e3:4c **Security**: Yes	**8**	E_Port

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. Others wise, 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 ASCI 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, Switch_2, HBA1, and JBOD 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

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_2 and Switch_1 as members.**

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

5. **Save and activate Security_Set_2 on Switch_2.**

Security Example: RADIUS Server

Consider the fabric shown in FIGURE 2-10. This fabric is similar to the one shown in FIGURE 2-9 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 2-10 Security Example: RADIUS Server

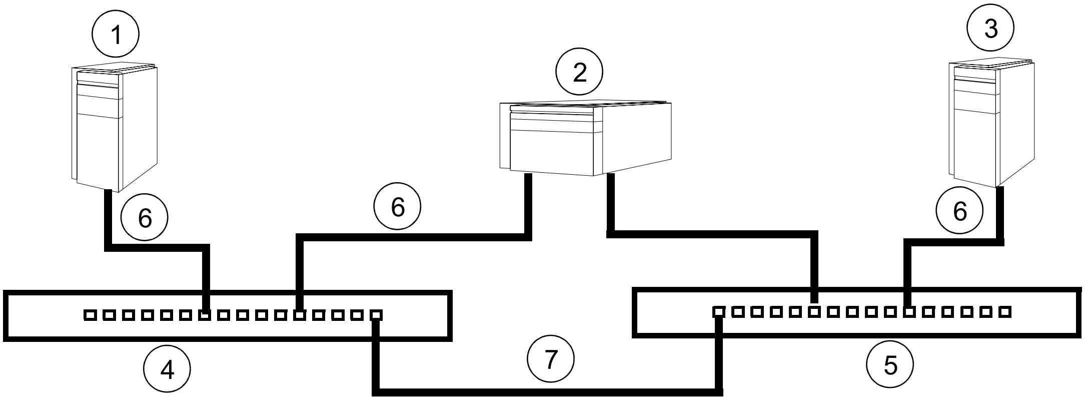


Figure Legend

1	**Device**: HBA_1 **WWN**: 10:00:00:c0:dd:07:c3:4d **Security**: Yes	5	**Device**: Switch_2 **WWN**: 10:00:00:c0:dd:07:e3:4e **Security**: Yes
2	**Server**: Radius_1 **IP Address**:10:20:30:40	6	F_Port
3	**Device**: HBA_2 **WWN**: 10:00:00:c0:dd:07:c3:4f **Security**: No	7	E_Port
4	**Device**: Switch_1 **WWN**: 10:00:00:c0:dd:07:e3:4c **Security**: Yes		

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 ASCI 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. Others wise, 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 ASCI 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 2-11. 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 2-11 Security Example: Management Server

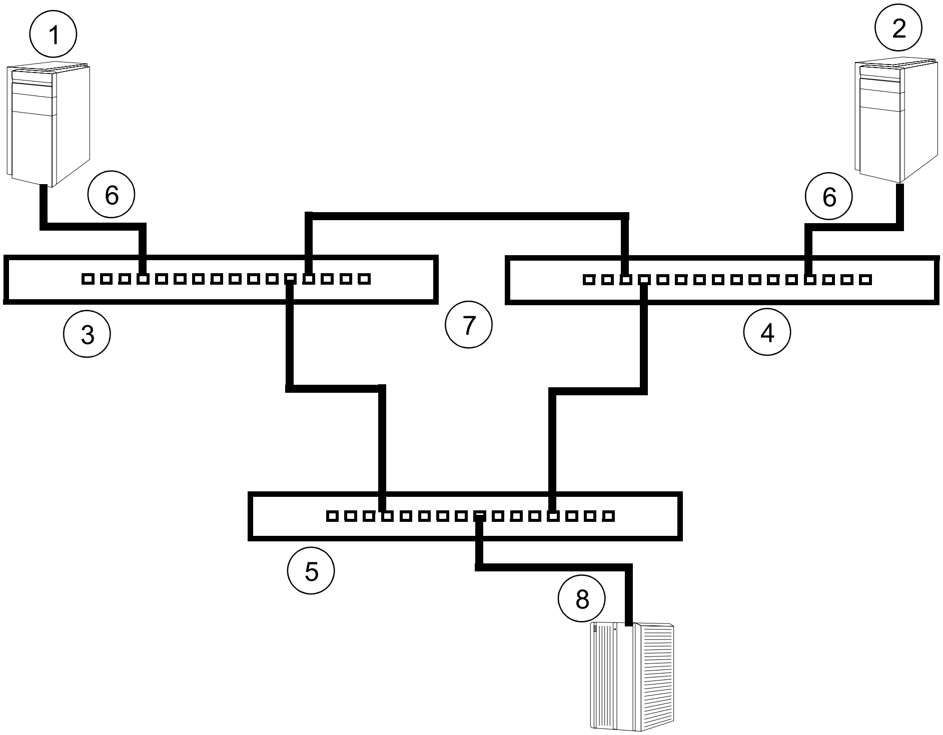


Figure Legend

1	**Device**: HBA_1/APP_1 **Security**: No	**5**	**Device**: Switch_3 **Security**: No
2	**Device**: HBA_2/APP_2 **WWN**: 10:00:00:c0:dd:07:c3:4d **Security**: Yes	**6**	F_Port
3	**Device**: Switch_1 **Security**: No	**7**	E_Port
4	**Device**: Switch_2 **WWN**: 10:00:00:c0:dd:07:e3:4e **Security**: Yes	**8**	FL_Port

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.

MS Group: Group_1	
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 and provides for the configuration, control, and maintenance of multiple fabrics. Supported platforms include Windows, Solaris, or Linux.

The browser-based application, QuickTools and the CLI reside in the switch firmware and provide for the management of individual switches in a single fabric. Consider how many fabrics and switches 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 that are reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for Enterprise Fabric Suite 2007 logins, QuickTools logins, Application Programming Interface (API) logins, and Telnet logins.

Additional logins will be refused.

CHAPTER 3

Installation

This chapter describes how to install and configure the switch. The following topics are covered:

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

Site Requirements

Consider the following items when installing a Sun Storage Fibre Channel Switch 5802:

- Fabric Management Workstation
- Switch Power Requirements
- Environmental Conditions

Fabric Management Workstation

The requirements for fabric management workstations are described in TABLE 3-1:

TABLE 3-1 Management Workstation Requirements

Component	Requirement
Operating System	• Windows 2003 and XP SP1/SP2 • Solaris 9, 10, and 10 x86 Operating System • Red Hat Enterprise Linux 4 and 5 • SUSE Linux Enterprise Server 9 and 10
Memory	512 MB or more; 1 GB recommended
Processor	1 GHz or faster
Internet Browser	Microsoft Internet Explorer 6.0 or later Netscape Navigator 6.0 and later Mozilla 1.5 and later Firefox 1.5 and later Java 2 Standard Edition Runtime Environment 1.4.2 for QuickTools

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

Switch Power Requirements

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

Environmental Conditions

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

- Operating temperature range: 5–40°C (41–104°F)
- Relative humidity: 10–90%, non-condensing

Installing a Switch

Installing a switch involves the following steps:

1. Verify the Package Contents
2. Mount the Switch
3. Stack Switches
4. Install Transceivers
5. Apply Power to the Switch
6. Configure the Workstation
7. Connect the Workstation to the Switch
8. Configure the Switch
9. Connect Devices and Switches

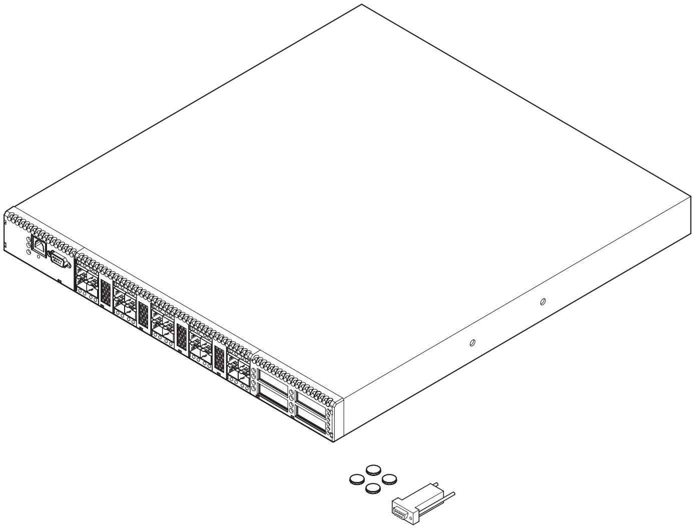
Verify the Package Contents

Unpack the switch and accessories. The Sun Storage Fibre Channel Switch 5802 product is shipped with the components shown in FIGURE 3-1:

- Sun Storage Fibre Channel Switch 5802 Fibre Channel Switch (1) with firmware installed
- DB9-to-RJ-45 Adapter (1)
- Rubber feet (4)

Note – If you ordered SFPs and XPAK switch stacking cables, they will arrive in a different package. XPAK switch stacking cables connect switches together through the XPAK ports.

FIGURE 3-1 Sun Storage Fibre Channel Switch 5802



Mount the Switch

The switch can be placed on a flat surface and stacked, or mounted in one of the following cabinets:

- Sun StorEdge 72-Inch Expansion cabinet
- Sun Rack 900 and 1000 cabinets
- Any 19” standard Electronics Industries Association (EIA) rack

Adhesive rubber feet are provided for surface mounts. Without the rubber feet, the switch occupies 1U of space. See “Dimensions” on page 80 for weight and dimensional specifications.

Rack mounting requires the Sun Storage Fibre Channel Switch 5802 rail kit, which you must purchase separately. For instructions about how to install the rail kit, see the *Sun Storage Fibre Channel Switch 5802 Rack Mounting Guide* that is packaged with the rail kit.

Caution – 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.

Caution – If the switch is mounted in a closed or multi-rack assembly, the operating temperature of the rack environment may be greater than the ambient temperature. Be sure to install the chassis in an environment that is compatible with the maximum rated ambient temperature. Refer to “Environmental” on page 81 for technical specifications.

Caution – Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the switch (surface mount) or rack for service access and ventilation.

Caution – 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” on page 81.

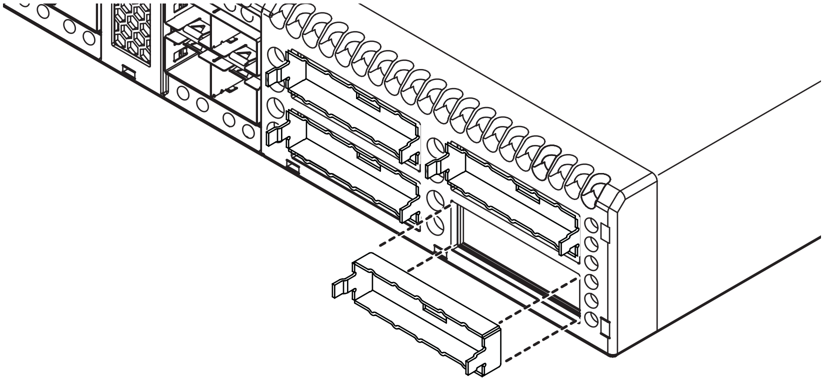
Caution – eliable grounding in the rack must be maintained from the switch chassis to the AC power source.

Stack Switches

Caution – To maintain proper air flow and prevent the switch from overheating, keep covers installed in unused XPAK ports.

You can connect up to six switches together through the XPAK ports using XPAK switch stacking cables. Stacking provides performance and fail-over while preserving ports for devices. Refer to "Stacking" on page 22 for more information. If you are using the XPAK ports, remove the port covers by the cover tabs using your fingers or pliers as shown in FIGURE 3-2.

FIGURE 3-2 Removing XPAK Port Covers



To install XPAK switch stacking cables, position the cable connectors with the circuit board toward the mid line of the respective switch faceplates as shown in FIGURE 3-3. When installing the 3-inch XPAK switch stacking cable, insert the cable connectors into the XPAK ports at the same time.

FIGURE 3-3 Installing XPAK Switch Stacking Cables

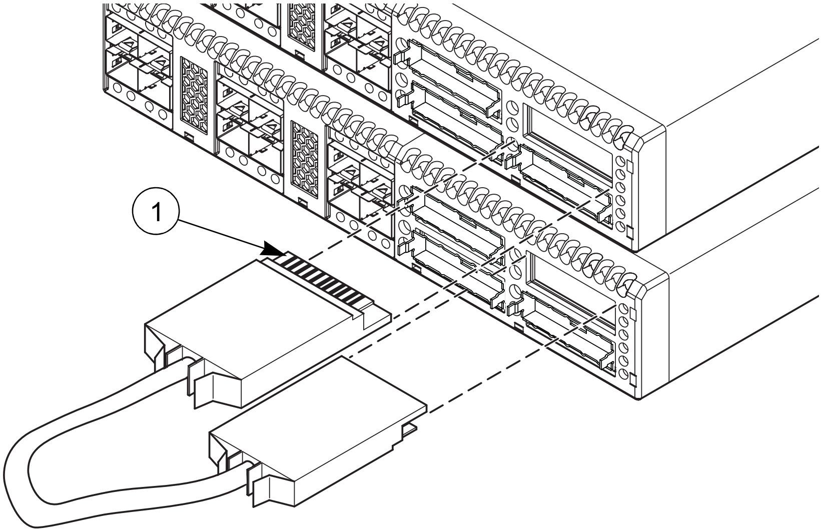


Figure Legend

1	Circuit Board

Install Transceivers

The switch supports a variety of SFP and XPAK transceivers. To install a transceiver, wear an Electrostatic Sensitive Device (ESD) wrist strap connected to ground and insert the transceiver into the switch port; gently press the transceiver until it snaps in place. To remove a transceiver, gently press the transceiver into the port to release the tension, then 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.

Apply Power to the Switch

Caution – This product requires a 3-wire power cable and plug 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.

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

The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by UL and CSA.
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

To power up the switch, connect the power cords to the power supply receptacles on the back of the switch chassis and to a grounded AC outlet. To provide redundancy in the event of an AC power circuit failure, connect the switch power supplies to separate AC circuits.

The switch responds in the following sequence:

1. The chassis LEDs (Input Power, Status (OK), System Fault) illuminate followed by all port Logged-In LEDs.
2. After a couple seconds the System Fault LED is extinguished while the Input Power LED and Status (OK) LED remain illuminated.
3. After approximately one minute, the POST executes and the Status (OK) LED is extinguished.
4. After about another minute, the POST is complete, all LEDs are extinguished except the Input Power LED and the Status (OK) LED:
   - The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.
   - The Status (OK) LED indicates the results of the POST. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry. If the Status (OK) LED illuminates continuously, the POST was successful, and you can continue with the installation process.

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 QuickTools or Enterprise Fabric Suite 2007 to manage the switch, the Configuration Wizard manages the workstation IP address for you – proceed to "Connect the Workstation to the Switch" on page 53.

Configuring the Workstation IP Address for Ethernet Connections

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

For a Windows workstation:

1. **Click the Start button and 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 OS workstation:

Open a command window and enter the following command where (interface) is your interface name:

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

Configuring the Workstation Serial Port

To configure the workstation serial port, do the following:

1. **Connect a null modem F/F DB9 cable from a COM port on the management workstation to the RS-232 serial port on the switch.**
2. **Configure the workstation serial port according to your platform:**

For Windows:

1. **Open the HyperTerminal application. Choose the Start button, select Programs, Accessories, HyperTerminal, and HyperTerminal.**
2. **Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the OK button.**
3. **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:

1. **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
   ```

2. **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 OS:

Modify the /etc/remote file to include the following lines. /dev/term/a refers to serial port a. Choose the "dv" setting to match the workstation port to which you connected to the switch.

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

Connect the Workstation to the Switch

You can manage the switch using the CLI, QuickTools, or Enterprise Fabric Suite 2007. QuickTools and Enterprise Fabric Suite 2007 require an Ethernet connection to the switch. The CLI can use an Ethernet connection or a serial connection. 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.
- Serial port connection from the management workstation to the switch RJ-45 serial port connector on the switch. This requires the DB9-to-RJ-45 adapter provided with the switch and a 10/100 Base-T straight cable.

Configure the Switch

You can configure the switch using the CLI, QuickTools, or Enterprise Fabric Suite 2007. Enterprise Fabric Suite 2007 is an optional, full fabric graphical user interface. Refer to the *Enterprise Fabric Suite 2007 User Guide* for information about installing Enterprise Fabric Suite 2007.

QuickTools Switch Configuration

To log in and configure the switch using QuickTools, do the following:

1. **Open an Internet browser and enter the default IP address `10.0.0.1` to start the QuickTools web applet.**

2. **Log in to the switch using the default user name (`admin`) and password (`password`).**

3. **Obtain the IP address and subnet mask from your network administrator.**

4. **Open the QuickTools Wizards menu and select Configuration Wizard. Follow the instructions to set the switch IP address and the password. Changing the IP address will terminate the QuickTools session.**

5. **Open an Internet browser again and log in with the new IP address.**

CLI Switch Configuration

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 default account name and password (admin/password).

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

Note – To ensure user account security, you should change the password for the Admin account name. Refer to the Passwd command in the *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide*

   - 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 OS: 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). Refer to the** *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* **for more information about the CLI commands.**

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

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

Connect Devices and Switches

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.

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

Installing Firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the CLI, QuickTools, or Enterprise Fabric Suite 2007 to install new firmware. This guide describes how to install firmware using QuickTools and the CLI. Refer to the *Enterprise Fabric Suite 2007 User Guide* for information about installing firmware using Enterprise Fabric Suite 2007.

- Using QuickTools to Install Firmware
- Using the CLI to Install Firmware

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

- The current firmware version 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 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 Firmware Upload dialog, click the Browse button to browse and select the firmware file to be uploaded.**
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. **QuickTools prompts you to activate the new firmware using a hot (non-disruptive) reset, if possible. Click the OK button to reset the switch and activate the new firmware.**

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 57.
- 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 58.

Refer to the *Sun Storage Fibre Channel Switch 5802 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 *Sun Storage Fibre Channel Switch 5802 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.**

```
Switch #> admin start
Switch #> firmware install
The switch will be reset. This process will cause a disruption to
I/O traffic.
Continuing with this action will terminate all
managementsessions,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 : 7.4.x.xx.xx_epc
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).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
```

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

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

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 non-disruptive (Hotreset command). The following example illustrates a custom firmware installation with a non-disruptive 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:

     ```
     Switch (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.

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

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

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

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

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

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

```
Switch (admin) $>image unpack filename
```

4. **Wait for the unpack to complete.**

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

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

```
Switch (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 use 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 19 for information about available license keys. To install a license key using QuickTools, 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 *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide*.

CHAPTER 4

Diagnostics/Troubleshooting

Diagnostic information about the switch is available through the chassis LEDs and the port LEDs. Diagnostic information is also available through the CLI, QuickTools, or Enterprise Fabric Suite 2007 event logs and error displays. This chapter describes the following types of diagnostics:

- Chassis Diagnostics describes the Input Power LED and System Fault LED indications.
- Power-On Self Test Diagnostics describe the Status (OK) LED and the port Logged-In LED indications.
- Power Supply Diagnostics describes Power Supply Status LED and Power Supply Fault LED indications.

This section also describes using maintenance mode to recover a disabled switch.

Chassis Diagnostics

Chassis diagnostics are indicated by the chassis LEDs as shown in FIGURE 4-1.

FIGURE 4-1 Chassis LEDs

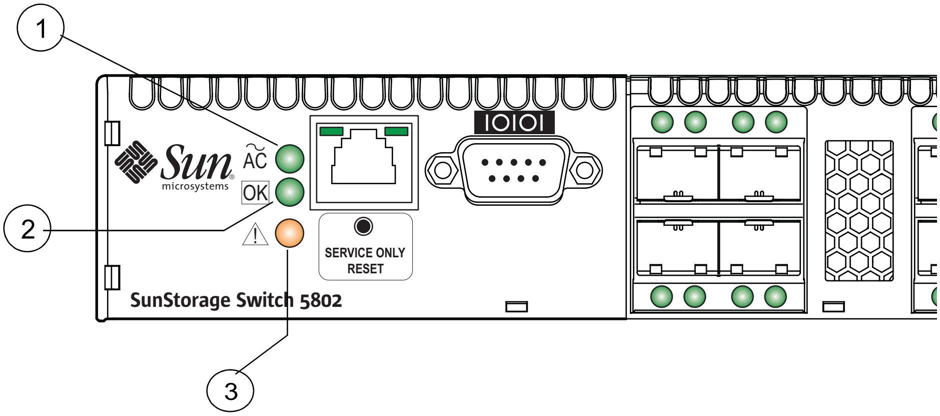


Figure Legend

1	Input Power LED (Green)
2	Status (OK) LED (Green)
3	System Fault LED (Amber)

The following conditions are described:

- Input Power LED Is Extinguished
- System Fault LED Is Illuminated

Input Power LED Is Extinguished

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

1. **Inspect the power cords and connectors. Is the cord unplugged? Is the cord or connector damaged?**
   - Yes - Make necessary corrections or repairs. If the condition remains, continue.
   - No - Continue.

2. **Inspect the AC power source. Is the power source delivering the proper voltage?**
   - Yes - Continue.
   - No - Make necessary repairs. If the condition remains, continue.
3. **Inspect the power supplies. Are the power supplies fully seated in their bays?**
   - Yes - Continue. Replace the power supplies.
   - No - Reinstall the power supplies. If the condition remains, replace the power supplies.

System Fault LED Is Illuminated

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. If the System Fault LED illuminates, do the following:

- If the Status (OK) LED is illuminated also, check the power supply LEDs and take the necessary actions. For specific instructions, see "Power Supply Diagnostics" on page 68.
- If the Status (OK) LED is extinguished, contact your authorized maintenance provider.

Power-On Self Test Diagnostics

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

- Checksum tests on the boot firmware in Programmable Read Only Memory (PROM) and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the Application Specific Integrated Circuit (ASIC)

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

If there are no errors, the Status (OK) LED illuminates continuously. If a critical error occurs, the Status (OK) LED will be extinguished and the System Fault LED will illuminate. If there are non-critical errors, the switch disables the failed ports and flashes the associated Logged-In LEDs.

Logged-In LED Indications

Port diagnostics are indicated by the Logged-In LED for SFP and XPAK ports as shown in FIGURE 4-2.

FIGURE 4-2 Logged-In LED

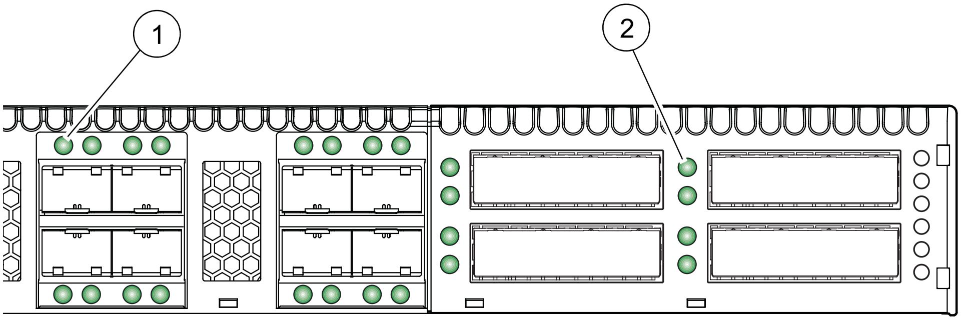


Figure Legend

1	SFP Port Logged-In LED
2	XPAK Port Logged-In LED

The Logged-In LED has three indications:

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

If a Logged-In LED is flashing twice per second, review the event browser for alarm messages regarding the affected port. You can also inspect the alarm log using the Show Alarm command. If there is an error, alarm messages may 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. E_Port isolation can be caused by the following:

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

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

1. **Does the event browser show an alarm about an invalid attach on the affected port?**
   - Yes - If device security is configured, 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 click the Switch tab and Summary icon in QuickTools. 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. 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 click the Switch tab and Advanced icon in QuickTools. Is each timeout value the same on every switch?**
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch CLI. Reset the port. If the condition remains, continue.
5. **Display the active zone set on each switch using the Zoning Active command, or click the Active Zoneset tab in QuickTools. 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, then reset the port. If the condition remains, contact your authorized maintenance provider.

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

Excessive Port Errors

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

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

Port threshold alarm monitoring is disabled by default. Refer to the *Sun Storage Fibre Channel Switch 5802 Command Line Interface 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
- Faulty device or HBA

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

1. **Examine the alarm configuration for the associated error using the Show Config Threshold command. Refer to the Show Config Threshold command in the** *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide***. Are the thresholds and sample window correct?**
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.

2. **Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the** *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* **or the** *Sun Storage Fibre Channel Switch 5802 QuickTools Switch Management User Guide* **for information about testing ports. 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 Diagnostics

A power supply has a Status LED (Green) and a Fault LED (Amber) as shown in FIGURE 4-3. Under normal operating conditions, the Power Supply Status LED is illuminated and the Power Supply Fault LED is extinguished.

FIGURE 4-3 Power Supply LEDs

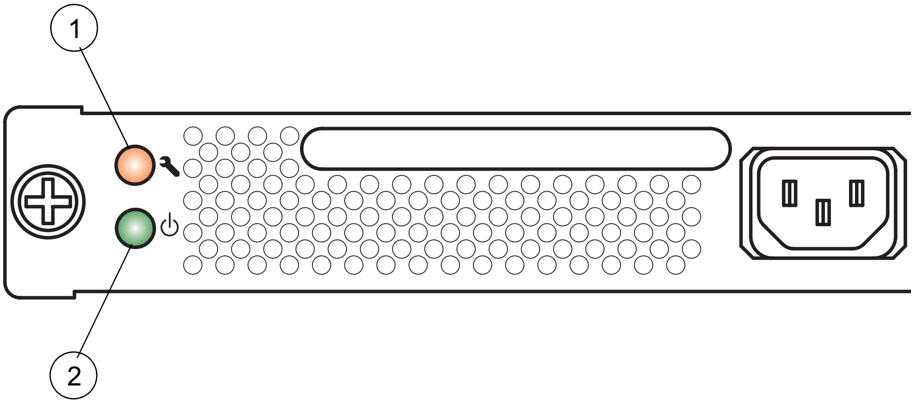


Figure Legend

1	Power Supply Fault LED
2	Power Supply Status LED

Consider the following indications:

- All power supply LEDs are normal, yet the System Fault LED and the Status (OK) LED are illuminated. This means that the two power supplies have different air flow directions. Replace the power supply with the incorrect air flow direction with another having the correct air flow direction. Air flow direction is marked on the power supply part number label. Refer to "Power Supply Removal and Replacement" on page 74.
- Power Supply Fault LED is illuminated. This means that the power supply is failing or has failed. Replace the power supply with another having the same air flow direction. Air flow direction is indicated on the power supply part number label. Refer to "Power Supply Removal and Replacement" on page 74.

Recovering a Switch Using Maintenance Mode

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

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

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

- Exiting the Maintenance Menu (Option 0)
- Unpacking a Firmware Image File in Maintenance Mode (Option 1)
- Resetting the Network Configuration in Maintenance Mode (Option 2)
- Resetting User Accounts in Maintenance Mode (Option 3)
- Copying Log Files in Maintenance Mode (Option 4)
- Removing the Switch Configuration in Maintenance Mode (Option 5)
- Remaking the File System in Maintenance Mode (Option 6)
- Resetting the Switch in Maintenance Mode (Option 7)
- Updating the Boot Loader in Maintenance Mode (Option 8)

To recover a switch, do the following:

1. **Place the switch in maintenance mode. Press and hold the Maintenance button with a pointed tool until the Status (OK) LED is extinguished, and then release the button. The Status (OK) LED flashes in maintenance mode.**

2. **Establish a Telnet session with the switch using the maintenance mode IP address `10.0.0.1`.**

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

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

4. **The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press 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 Switch
8)  Update Boot Loader
Option:
```

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

Exiting the Maintenance Menu (Option 0)

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

Unpacking a Firmware Image File in Maintenance Mode (Option 1)

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

1. **Place the switch in maintenance mode. Refer to the procedure for maintenance mode in** “Recovering a Switch Using Maintenance Mode” on page 69**.**

2. **Use FTP to load a new firmware image file onto the switch. Refer to** “Custom Firmware Installation” on page 58 **for an example of how to load the image file. When the download is complete, close the FTP session.**

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

   ```
   telnet 10.0.0.1
   ```

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

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

5. **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.
   ```

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

Resetting the Network Configuration in Maintenance Mode (Option 2)

The Reset Network Config option resets the network properties to the factory default values and saves them on the switch. Refer to *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for the default network configuration values.

Resetting User Accounts in Maintenance Mode (Option 3)

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

Copying Log Files in Maintenance Mode (Option 4)

The Copy Log Files option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation, however, you must download the logfile before resetting the switch. Refer to the *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for information about downloading files from the switch.

Removing the Switch Configuration in Maintenance Mode (Option 5)

The Remove Switch Config option deletes all configurations from the switch except the default configuration. This restores switch configuration parameters to the factory defaults. Refer to Reset command in the *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for the factory default values.

Remaking the File System in Maintenance Mode (Option 6)

In the event of a loss of power, the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. The Remake Filesystem option resets the switch to the factory default values, including user accounts and zoning. Refer to the Reset command in the *Sun Storage Fibre Channel Switch 5802 Command Line Interface Guide* for the factory default values.

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 the Switch in Maintenance Mode (Option 7)

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

Updating the Boot Loader in Maintenance Mode (Option 8)

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

CHAPTER **5**

Removal/Replacement

This chapter describes the removal and replacement procedures for the following field replaceable units (FRU):

- SFP and XPAK transceivers
- Power supplies

The switch is equipped with a battery that powers the non-volatile memory. This memory stores the switch configuration. The battery is not a field replaceable unit.

Caution – Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of the used battery according to the manufacturer’s instructions.

Transceiver Removal and Replacement

The SFP and XPAK transceivers can be removed and replaced while the switch is operating without damaging the switch or the transceiver. However, data transmission on the affected port will be interrupted until the transceiver installed.

To remove a transceiver, gently press the transceiver into the port to release the tension, then 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.

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

Power Supply Removal and Replacement

The power supplies are hot pluggable. This means you can remove or install one of the power supplies while the switch is operating without disrupting service. The power supplies are also interchangeable; that is, the left and right power supplies are the same unit.

Caution – Both power supplies must have the same air flow direction to prevent the switch from overheating.
To avoid overheating, do not operate the switch with one power supply any longer than necessary.

When removing or replacing a power supply, consider the following:

- The left and right power supplies are interchangeable. However, you must orient the power supply so that AC receptacle is on the right.
- Both power supplies must have the same air flow direction. The part number label on the power supply indicates the air flow direction.
- When removing or replacing a power supply on an operating switch, be sure the Status (OK) LED is illuminated. This allows the switch to correctly report power supply status.

To remove a power supply, unplug the power supply and loosen the two fasteners with a cross-head screw driver as shown in FIGURE 5-1. Grasp the power supply handle and pull firmly to disengage the modular connector. Slide the power supply out of its bay.

FIGURE 5-1 Power Supply Removal

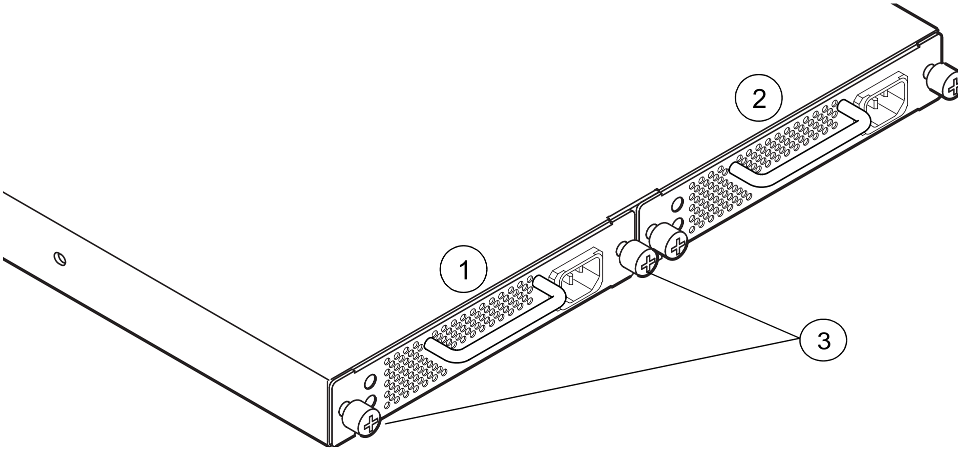


Figure Legend

1	Power Supply 1
2	Power Supply 2
3	Fasteners

1. **Confirm that the Status (OK) LED is illuminated. This allows the switch to correctly report power supply status.**

2. **Confirm that the new power supply is compatible with the switch air flow direction. The part number label on the power supply indicates the air flow direction as shown in** FIGURE 5-2**.**

3. **With the AC receptacle on the right, slide the power supply into the bay until it is firmly seated. Secure the knurled fasteners by hand.**

4. **Plug the power cord into the AC receptacle. Confirm that air flow is correct.**

FIGURE 5-2 Power Supply Removal

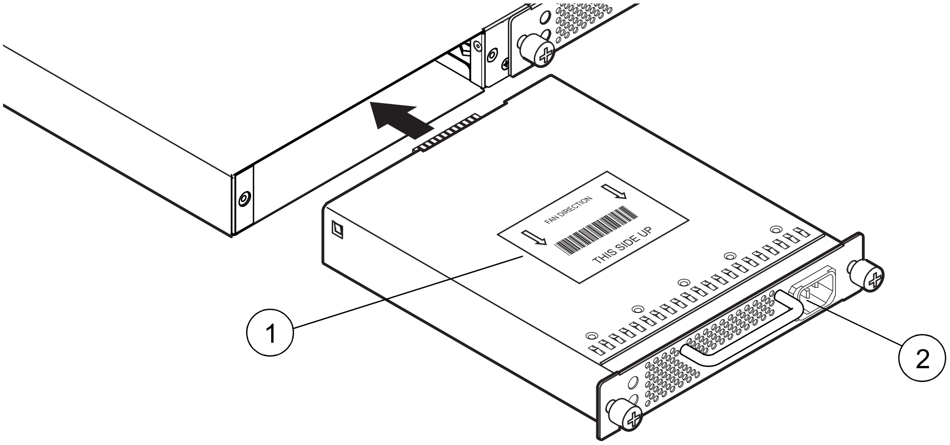


Figure Legend

1	Air Flow Label
2	AC Receptacle

APPENDIX **A**

Specifications

This appendix contains the specifications for the Sun Storage Fibre Channel Switch 5802 Fibre Channel switch. Refer to Chapter 1 for the location of all connections, switches, controls, and components.

- Fabric Specifications
- Maintainability
- Fabric Management
- Dimensions
- Electrical
- Environmental
- Regulatory Certifications

Fabric Specifications

TABLE A-1 Fabric Specifications

Fibre Channel Protocols	FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-DA FC-FLA FC-FS-2 FC-GS-5 FC-FG FC-LS FC-MI-2 FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-PI-3 FC-SP FC-Tape FC-VI FC-SW-4 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service	Classes 2 and 3
Modes of Operation	Fibre Channel Classes 2 and 3, connectionless
Port Types	
• SFP Ports	G_Port, GL_Port, F_Port, FL_Port, E_Port
• XPAK Ports	G_Port, F_Port, E_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	8, 12, 16, or 20 SFP ports Four XPAK ports
Scalability	Maximum 239 switches depending on configuration
Maximum User Ports	> 475,000 ports depending on configuration
Buffer Credits	16 buffer credits per port, ASIC embedded memory

TABLE A-1 Fabric Specifications *(Continued)*

Media Type	
Ports 0-19	SFP optical transceiver
Ports 20-23	XPAK switch stacking cables
Fabric Port Speed	
Ports 0-19	1.0625, 2.125, 4.250, or 8.50 Gbps
Ports 20-23	12.750 or 25.50 Gbps
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	400 MHz 440EP processor
Fabric Latency (intra-switch)	
2-Gbps to 2-Gbps	< 0.6 µsec
4-Gbps to 4-Gbps	< 0.3 µsec
8-Gbps to 8-Gbps	< 0.2 µsec
10-Gbps to 10-Gbps	< 0.2 µsec
20-Gbps to 20-Gbps	< 0.2 µsec
Bandwidth	
Point-to-Point	425 MB, Full Duplex @ 2-Gbps 850 MB, Full Duplex @ 4-Gbps 1700 MB, Full Duplex @ 8-Gbps 2550 MB, Full Duplex @ 10-Gbps 5100 MB, Full Duplex @ 20-Gbps
Aggregate (single switch)	Up to 54.40 GB Full Duplex

Maintainability

TABLE A-2 Maintainability Specifications

Diagnostics	Power-On Self Test (POST) tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User Interface	LED indicators
Field Replaceable Units	Power supplies

Fabric Management

TABLE A-3 Fabric Management Specifications

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

Dimensions

TABLE A-4 Dimensional Specifications

Width	17″ (432 mm), 19 inch rack mount
Height	1.70″ (43.2 mm) (1U)
Depth	19.69″ (500 mm)
Weight	18 lbs (8.16 Kg)

Electrical

TABLE A-5 Electrical Specifications

Operating voltage	100 to 240 VAC; 50 to 60 Hz
Power source loading (maximum)	1 A at 120 VAC 0.5 A at 240 VAC
Heat Output (maximum)	120 watts
Circuit Protection	Internally fused

Environmental

TABLE A-6 Environmental Specifications

Temperature	
• Operating	5 to 40°C (41 to 104°F)
• Non-operating	-20 to 70°C (-4 to 158°F)
Humidity	
• Operating	10% to 90%, non-condensing
• Non-operating	10% to 95%, non-condensing
Altitude	
• Operating	0 to 3048 m (0 to 10,000 feet)
• Non-operating	0 to 15,240 m (0 to 50,000 feet)
Vibration	IEC 68-2-6,5
• Operating	5 - 500 Hz, 0.2 g, 3 axis, dwell
• Non-operating	2 - 200 Hz, 0.6 g, 3 axis, dwell
Shock	IEC 68-2
• Operating	4 g, 11 ms, half sine, 20 repetitions/axis
• Non-operating	30 g, 13 msec., 3 axis
Air flow	Front-to-back or back-to-front

Regulatory Certifications

TABLE A-7 Regulatory Certifications

Safety Standards	UL 60950-1 (USA) cUL 60950-1 (Canada) DEMKO and GS EN60950-1:2001, CE (Europe) CB Scheme: IEC 60950-1 (2001) GOST-R (Russia)
Emissions Standards	FCC Part 15 Class A ICES-003 Issue 4 VCCI Class A ITE CISPR 22, Class A EN 55022, Class A AS/NZS CISPR 22
Voltage Fluctuations	EN 61000-3-3
Harmonics	EN 61000-3-2
Immunity	EN 55024
Marking	UL_{US} (United States) cUL (Canada) CE (Europe) UL/GS (Europe) DEMKO (Europe)

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 used to make defining zone set membership easier. 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. A chip designed for a specific applications, such as a transmission protocol or a computer.

BootP Boot Strap Protocol. A type of network server.

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

Cascade Topology A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

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 QuickTools wizard that automates the switch configuration process.

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

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

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

Enterprise Fabric Suite 2007 An optional 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 of Enterprise Fabric Suite 2007 that enables you to reallocate port buffer credits to extend transmission distances.

Fabric Database The set of fabrics that have been opened during a management 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 in QuickTools and Enterprise Fabric Suite 2007 associated with the file that contains user list data for the fabric.

Fabric Port An F_Port or FL_Port.

Fabric Security A feature that provides security for fabric users and devices including user account security and fabric services.

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

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).

Inband Management The ability to manage a switch through another switch over an inter-switch link.

Initiator The device that initiates a data exchange with a target device.

In-Order-Delivery A feature that requires that frames be received in the same order in which they were sent.

Input Power LED A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link The connection between two switches using E_Ports.

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 reset the switch or 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.

Mesh Topology A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB Management Information Base

Multistage Topology A fabric in which two or more edge switches connect to one or more core switches.

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.

Port Activation A licensed feature that enables you to activate additional FC ports.

Port Binding An authorization method that defines a list of device WWNs that can login to a switch port.

POST Power-On Self Test

Power-On Self Test Diagnostics that the switch chassis performs at start up.

Principal Switch The switch in the fabric that manages domain ID assignments.

QuickTools Browser-based switch management application that resides in the switch firmware.

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.

Simple Network Management Protocol An application protocol that manages and monitors network communications and functions. It also controls the Management Information Base (MIB).

Security Set A set of up to three groups with no more than one of each group type: ISL, Port, or MS. The active security set defines the device security for a 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

Stacking Cable An XPAK cable that you use to connect two or more switches through the 10-Gbps ports.

Status (OK) LED A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

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

Voluntary Control Council for Interference A consortium of Japanese electronics industry associations that have established voluntary standards for controlling electromagnetic interference (EMI).

Worldwide Name (WWN) A unique 64-bit address assigned to a device by the device manufacturer.

WWN Worldwide Name

XPAK A specification authored by a consortium of companies to govern the development of small form factor 10 and 20 Gigabit modules.

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.

Index