Compaq StorageWorks

Fibre Channel SAN Switch

Management Guide

First Edition (June 2000)
Part Number AA-RMMJA-TE / 207686-001
Compaq Computer Corporation

Notice

Compaq StorageWorks Fibre Channel SAN Switch Management Guide
First Edition (June 2000)
Part Number AA-RMMJA-TE / 207686-001

Contents

Chapter 3
Managing the Switch Using Web Management Tools

Chapter 4
Managing the Switch Using SNMP, Telnet, or Single Ethernet Port

Managing the Switch Using SNMP, Telnet, or Single Ethernet Port

continued

Chapter 5

Overview of the Fabric Operating System and QuickLoop

Chapter 6

Understanding and Using Zoning

Understanding and Using Zoning

continued

Chapter 7

Upgrading Firmware

Appendix A

Telnet Commands

Telnet Commands

continued

About This Guide

A Fibre Channel switch is used to interconnect storage devices, hosts, and servers in a Storage Area Network (SAN). There are several access methods for managing a switch. This guide is designed to be used as a tool for managing your switch.

Document Structure

This guide contains the following information:

Chapter 1: Overview

Switch management access methods

Chapter 2: Introducing StorageWorks Command Console

- Introduction to SWCC
- Where to find additional information about SWCC
- Installation requirements
- Installing SWCC for the Fibre Channel SAN Switch
- About Windows-based and Web-based management
- Accessing the SAN Interconnect Management home Web page

- Adding a new fabric
- Merging two fabrics
- Splitting a fabric

Chapter 7: Upgrading Firmware

- Rolling upgrades
- Upgrading firmware by using Web Management Tools, using a Telnet command, or downloading from the Compaq Website
- Save and restore switch configuration settings

Appendix A: Telnet Commands

- QuickLoop-specific commands
- Fabric Operating System and QuickLoop commands
- Zoning-specific commands

Glossary

Definition of terms

Related Documents

In addition to this guide, the following documentation may useful:

Table 2
Related Documents

Document Title	Part Number
Compaq StorageWorks™ Fibre Channel SAN Switch 8-EL Installation Guide	AA-RMMHA-TE 207687-001
Compaq StorageWorks™ Fibre Channel SAN Switch 8 Installation Guide	K-BCP24-IA. B01 (161355-002)
Compaq StorageWorks™ Fibre Channel SAN Switch 16 Installation Guide	EK-BCP28-IA. B01 (161356-002)
Compaq StorageWorks™ Command Console for Hubs, Switches, and Tape Controllers Getting Started Guide	AA-RHDAC-TE 135265-003
Compaq StorageWorks™ SAN Switch Remote Switch Services Installation Guide	EK-SANRS-AA. B01 165909-002

Text Conventions

This document uses the following conventions to distinguish elements of text:

Keys	Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously.
USER INPUT	User input appears in a different typeface and in uppercase.
Filenames	Filenames appear in italic, initial capital letters except when case-sensitive.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital letters.
COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in uppercase.
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to *enter* information, type the information and then press the **Enter** key.

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

Compaq Technical Support

In North America, call the Compaq Technical Phone Support Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for worldwide Technical Support Centers are listed on the Compaq website. Access the Compaq website at http://www.compaq.com.

Be sure to have the following information available before you call Compaq:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level
- Detailed, specific questions

Compaq Website

The Compaq website has information on this product as well as the latest drivers and Flash ROM images. You can access the Compaq website at http://www.compaq.com.

Compaq Authorized Reseller

For the name of your nearest authorized Compaq reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the Compaq website for locations and telephone numbers.

Chapter 1

Overview

A Fibre Channel switch is used to interconnect storage devices, hosts, and servers in a Storage Area Network (SAN). There are several access methods for managing a switch. Table 1-1 summarizes the different management access methods that are described in detail in this guide.

Table 1-1
Switch Management Access Methods

Method	Description	Local	In-Band*** (Fibre Channel)	Out-of-band (Ethernet)
Telnet*	Managed remotely using a TC/IP connection.	No	Yes	Yes
SNMP	Managed remotely using Simple Network Management Protocol	No	Yes	Yes
Web Management Tools	Managed remotely through the Web	No	Yes	Yes
StorageWorks Command Console (SWCC)	Managed remotely through SWCC software	No	Yes	Yes
Front Panel Controls**	Managed through the display screen located only on the Compaq StorageWorks SAN Switch 16	Yes	No	No

Note: *An advanced set of testing and debugging controls are available using a Telnet connection. Before a Telnet connection can be established the switch must have an IP address. To assign an IP address, refer to the installation guide that came with your Compaq *StorageWorks™ Fibre Channel SAN Switch*.

**Detailed information for managing the Compaq *StorageWorks™ Fibre Channel SAN Switch 16* from the front panel controls is included in the *Compaq StorageWorks Fibre Channel SAN Switch 16 Installation and Hardware Guide*.

***Most host bus adapters are not set up to initiate an in-band Fibre Channel IP connection. At least one switch must have an Ethernet connection. From that entry point you can manage the remaining switches in the fabric using in-band IP services.

Chapter 2

Introducing StorageWorks Command Console

Compaq *StorageWorks™ Command Console* (SWCC) software lets you manage your Fibre Channel SAN switches, fabrics, storage controllers, tape controllers and hubs from the Navigation window. When systems are added, they are displayed as icons in the Navigation window. Figure 2-1 shows the initial Navigation window, as it displays after starting SWCC immediately after installation.

The version of SWCC included with the switch lets you manage and monitor SAN elements using web-based, WBEM technology, or windows-based software. For the Fibre Channel SAN Switch, both management methods are installed during installation and are accessed from the SWCC Navigation window. The windows-based version supports many of the current Compaq StorageWorks products. The web-based version supports the new Fibre Channel elements that use Compaq WEBM technology.

Figure 2-1. Navigation window

Where to Find Additional Information About SWCC

This chapter provides a high-level overview of SWCC for the Fibre Channel SAN Switch. For more information on how to install and configure SWCC, refer to the following sources:

- SWCC Release Notes: Located in the SWCC folder on the CD included with the switch, the release notes are:
  - fcinter.txt –Provides information relating to the Fibre Channel Interconnect Agent and Fibre Channel Interconnect Client (web-based management),
  - Readme.txt –Provides information on software components, and installation,
  - ccclient.txt –Provides information relating to the Command Console Client, such as the Navigation window and tree.
- *Compaq StorageWorks Command Console for Hub, Switches, and Tape Controller Getting Started Guide*: Included in the switch kit, this document provides an overview of SWCC, SWCC setup requirements, detailed instructions on how to install and remove SWCC components, and troubleshooting information.
- Online Help: Online Help is available for both the windows-based and web-based versions of SWCC.

- Web Site: The web site for SWCC software and software support information is:

  http://www.compaq.com/products/storageworks/storage-management-software/command_console.html

SWCC Installation Requirements

SWCC software runs on Microsoft Windows NT 4.0, Service Pack 4 (or later), or Windows 2000 systems. SWCC requires a compatible network with TCP/IP and SNMP services installed on the host system. (Refer to Chapter 3 in the *SWCC Getting Started Guide* for instruction on how to install TCP/IP and SNMP services). For the web-based management support, SNMP services and a compatible web browser are required. Supported browsers are Explorer version 5.0 (or later), or Netscape Communicator version 4.6 (or later).

NOTE: SWCC does not support Dynamic Host Configuration Protocol (DHCP) or Windows Internet Name Service (WINS).

Installing SWCC for the Fibre Channel SAN Switch

1. Insert the CD into the CD-ROM drive. Navigate to the top-level SWCC directory and double-click setup.exe.
2. Follow the prompts. When the SWCC Setup screen (Figure 2-2) displays, if you want to install the client and agent on the same host, click the SAN Interconnect Devices and SAN Interconnect Management radio buttons. If you want to install just agent, only click the agent application SAN Interconnect Management radio button.

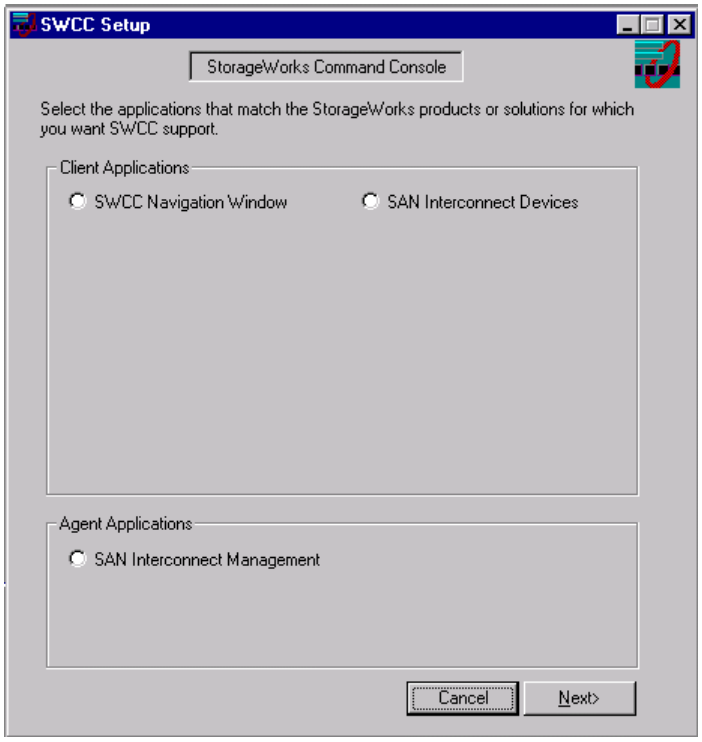


Figure 2-2. SWCC Setup Screen

3. Click Next on the SWCC Setup screen and continue with installation. During the installation, SWCC starts the Command Control Fibre Agent Configuration Utility (Figure 2-3). The utility prompts you to set the polling time. Enter a polling time in minutes and click Start.

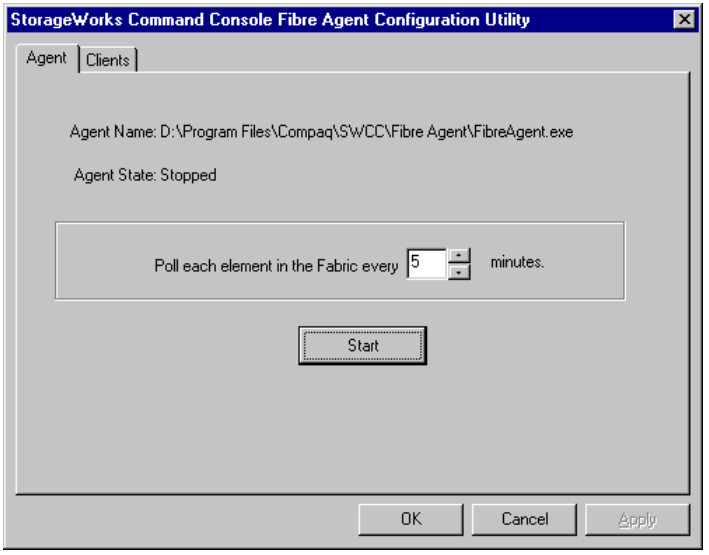


Figure 2-3. Fibre Agent Configuration Utility, Agent tab

4. Click the Clients tab (Figure 2-4). Enter the address of the client, and select TCP/IP and SNMP from the drop-down menu. This setting is required to install windows-based and web-based management support for the switch.

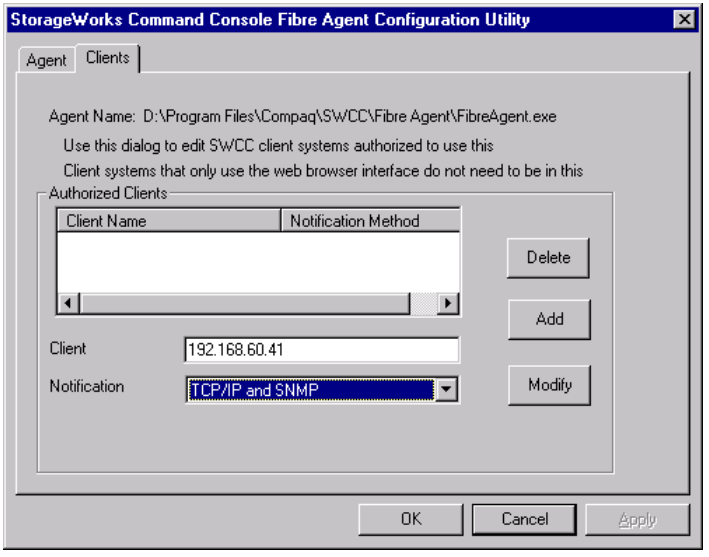


Figure 2-4. Fibre Agent Configuration Utility, Clients tab

5. Click OK to complete the installation.

Adding a System

1. From the Window 2000 or Windows NT Start menu, click Start > Programs > Command Console > StorageWorks Command Console to display the Navigation window.
2. From the File menu select Add System. When the Add System dialog box displays, enter the host name or address in the text box (Figure 2-5).

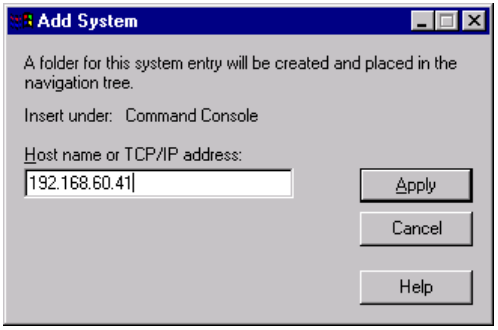


Figure 2-5. Add System dialog box

3. Click Apply. SWCC adds the system to the Navigation Window. Expand the folder for 192.168.60.41 (Figure 2-6). There are two icons: Fabric Window and Fabric Page. Double-click on the Fabric Window icon to follow the window-based software path, or the Fabric Page icon for the web-based management path.

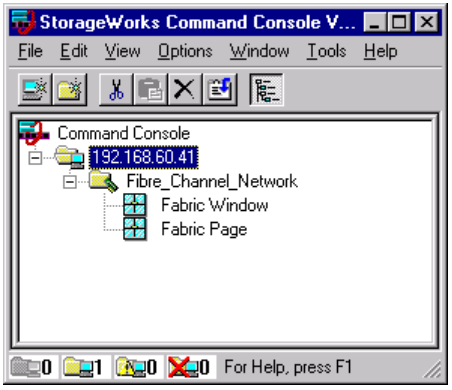


Figure 2-6. Navigation window, system added

About Windows-based Management

Fabric Window

The following is a generalized procedure to create a fabric and add fabric elements with windows-based management tools. Fabric and element names are user defined. The path begins by double-clicking the Fabric Window icon.

Creating a Fabric and Adding Fabric Elements

1. Double-click the Fabric Window icon. The first time you double-click on the icon the Add Fabric dialog box displays. Type in a fabric name in the text box. Click OK. SWCC creates the fabric and displays the Fabric Window (Figure 2-7). In this example, the fabric is named “demo.”

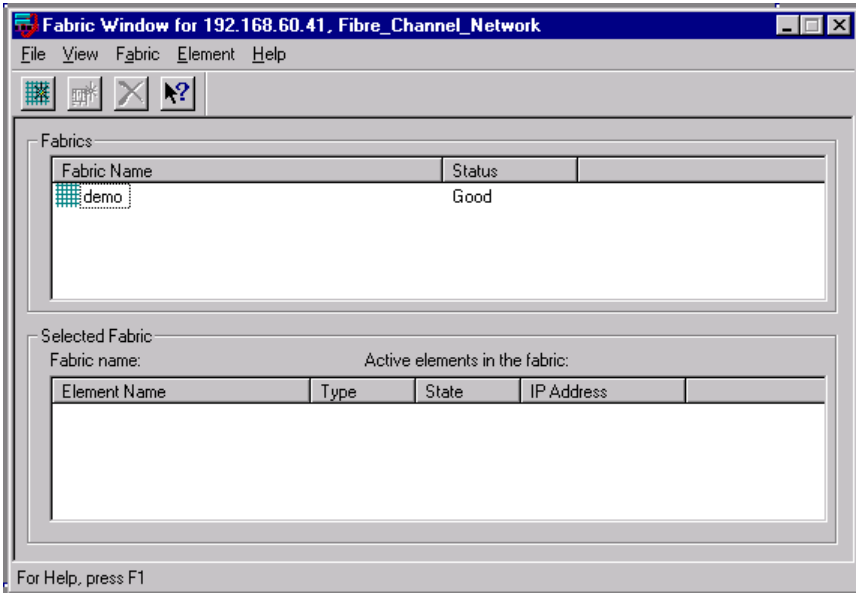


Figure 2-7. Fabric window

2. Highlight the demo icon. Choose Element > Add Element to display the demo: Add Element dialog box (Figure 2-8). Type the TCP/IP address of the switch and name it. Click OK.

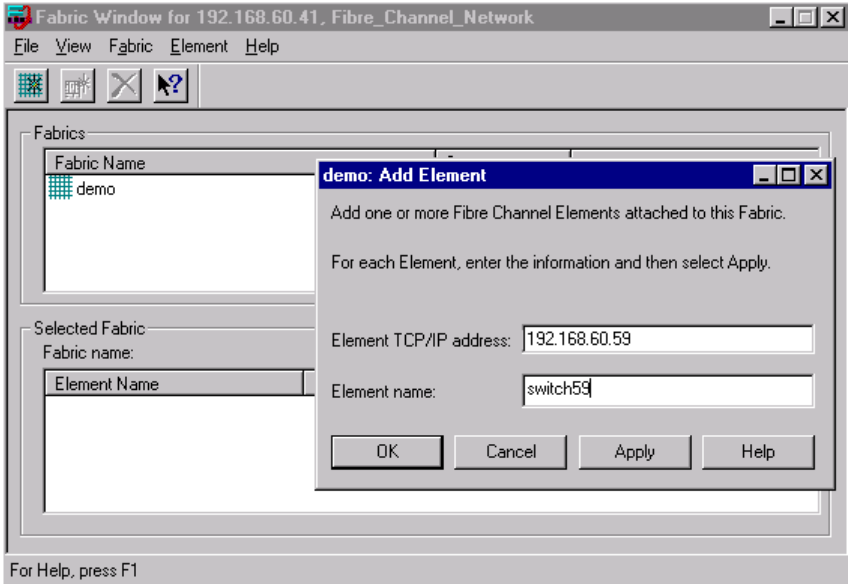


Figure 2-8. Add Element dialog box

Figure 2-9 shows the new fabric “demo” (in the top pane) and two switch elements (“switch59” and “switch47” in the bottom pane). Switch59 was added first; then switch47 was added.

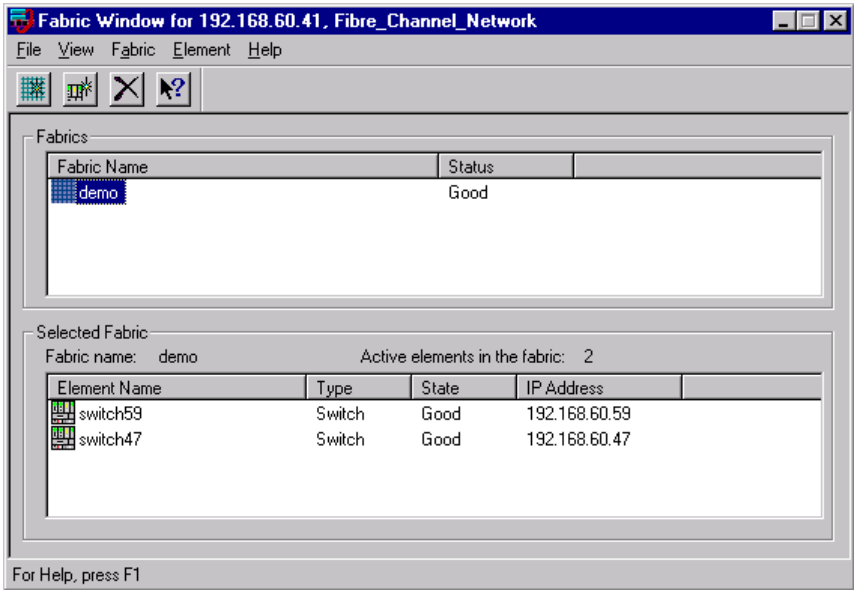


Figure 2-9. Fabric Window with switch elements added

3. To access switch management tools, double-click on a switch icon.

4. To access a view of all the switches in the fabric, right-click to see the switch menu and select TopZoneNS (Figure 2-10) to access the Fabric View.

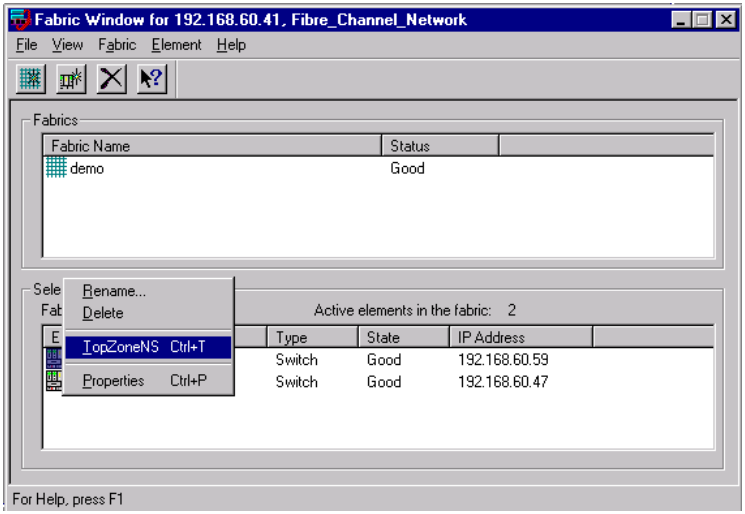


Figure 2-10. TopZoneNS selection

About Web-based Management

Fabric Page

Use this procedure to access SWCC web-based management support. The path begins by double-clicking on the Fabric Page icon, which displays a web page. Fabrics and fabric elements are monitored and managed using a standard web browser and single-click links. For procedures for defining fabrics and elements using web-based management, refer to online Help.

Viewing the Web-Based Management Pages

1. Double-click the Fabric Page icon and login to the Compaq Web-based Management page (Figure 2-11). See Table D-2 in the *SWCC Getting Started Guide* for passwords and account information.

2. Click the StorageWorks SAN Management link, the button on the left.

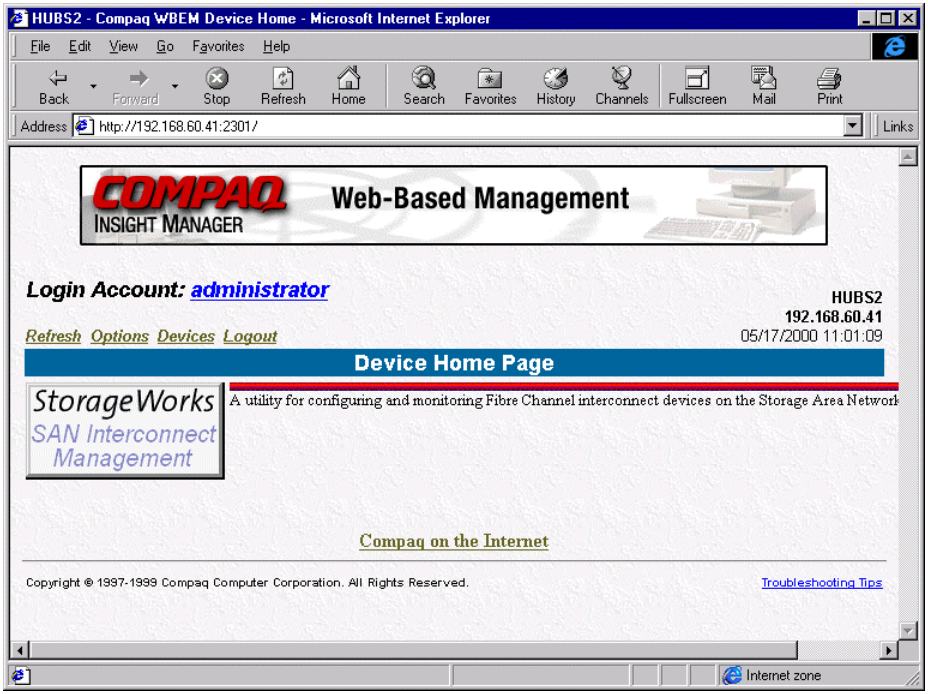


Figure 2-11. Web-Based Management home page

This link displays the SAN Interconnect Management V1.0 page (Figure 2-12). The left frame lists the fabrics. “Demo” is listed. The right frame lists the fabric elements. Switch59 and switch47 are listed.

3. Click a switch link to display the Switch Management Application page.
4. Click on TopZoneNS to display the Fabric View page.

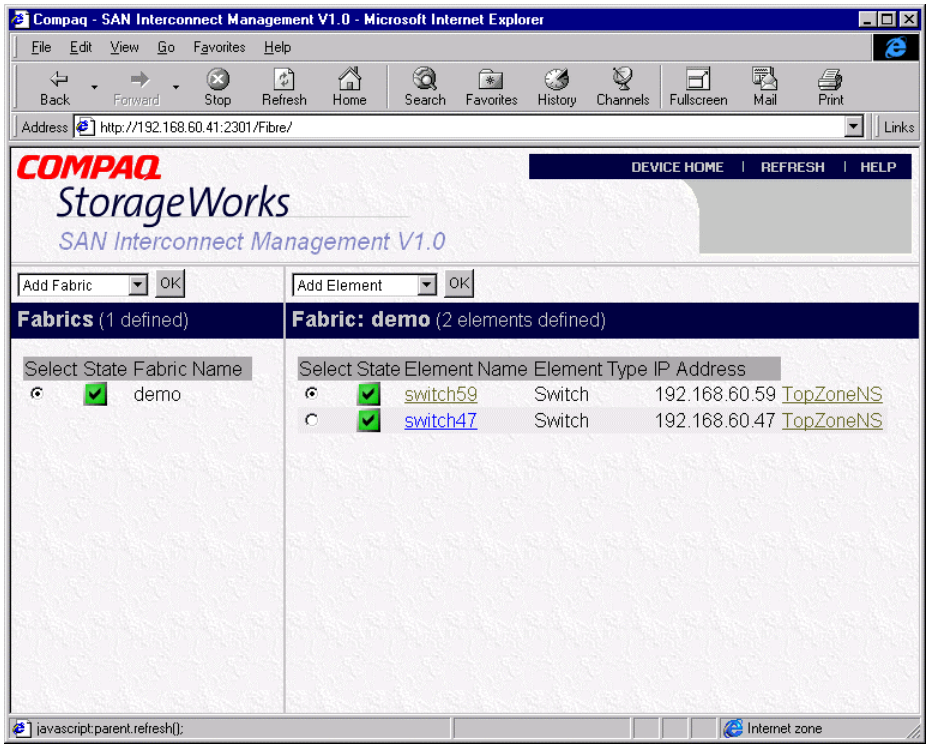


Figure 2-12. SAN Interconnect Management page

Accessing the SAN Interconnect Management Home Web Page

Once you have installed SWCC web-based support and a compatible browser, you can access the Compaq StorageWorks SAN Web-based Management page at:

http://agentsystemname:2301

Be sure to specify :2301 in the URL.

Chapter 3

Managing the Switch Using Web Management Tools

This chapter covers the following topics:

- Overview of Web Management Tools
  - Supported Web browsers
  - Java Plug-In software
  - Remote management features
  - User interface
  - Logging on to a switch
- User view pages
  - TopZoneNS page
  - Fabric Topology page
  - Switch Management Application page
  - Port Detail page
  - Performance page
  - Administrative Interface page
  - Telnet Interface page
- Useful information

Overview

Web Management Tools let you monitor and manage a SAN composed of Fibre Channel SAN Switches over the Web. Web Management Tools display information you can use to make overall topology decisions and administrative changes. You can interact dynamically with any switch in the SAN to monitor status and performance.

To manage the switch over the Web, launch SWCC (refer to *Compaq StorageWorks Command Console for Hubs, Switches, and Tape Controllers Getting Started Guide* for more information) or log on to a switch from a host with a Java-enabled Web browser.

Supported Web Browsers

Web Management Tools run on the following browsers:

- Internet Explorer 5.0 (or later) or Netscape 4.0 (or later) on systems with Windows NT or Windows 95
- Netscape 4.0 or later on systems with Solaris 2.5

NOTE: Netscape running on OpenVMS is not supported.

NOTE: The HotJava browser is not supported.

Java Plug-In Software

Java Plug-In software needs to be installed on your workstation to use Web Management Tools. The software eliminates troublesome behavioral differences between the two supported Web browsers, Netscape's Navigator and Microsoft's Internet Explorer. The plug-in software allows java applets used in the Web Management Tools program to run using Sun's Java Runtime Environment (JRE) instead of the browser's default java virtual machines. The JRE provides consistency and reliability when running applets. Java Plug-In works on other operating systems. For more information about Java Plug-In support for other operating systems, refer to the manual that came with your operating system. For more information on Java Plug-In, go to: http://java.sun.com/products/plugin/1.2/plugin.faq.html.

Remote Management Features

The Web Management Tools provide:

- Switch identification in the network
- Fabric topology and routing information
- Switch and port configuration control
- Real-time graphical switch and port status and statistics report
- User interface for zoning, name services, and QuickLoop
- Graphical representation of port performance (polled up to every 2.5 seconds depending on the operating system and browser used)
- Four minutes of aggregate bandwidth throughput shown graphically, scaled dynamically, and based on activity (polled up to every 2.5 seconds depending on the operating system and browser used)
- Secured management through the user interface or through a Telnet session
- Help functions including glossary help, online HTML help, and popup help for error conditions
- Out-of-band interface through a 10/100BaseT Ethernet connection
- In-band interface over a Fibre Channel link

Logging on to a Switch

To log on to a switch through the Web:

1. Launch a Web browser.
2. Connect to a switch by entering the URL or the Ethernet IP address for the switch. For example:

   http:\\switchname

   or

   http:\\IPAddress
3. Click the Admin button on the Switch Management Application page to access the administration screens. Enter your username and password at the prompt (see the "User Administration Page" section in this chapter for the default usernames and passwords).

User Interface

The Web Management Tools graphical user interface provides nine pages you can use to monitor and manage switch information. See Table 3-1.

Table 3-1
User Interface Screens

Pages	Description
TopZoneNS	Displays network switches and confirms World Wide Names (WWNs), domain Ids, and switch names.
Fabric Topology	Displays the physical configuration including active domains, paths, and routing information.
Name Server Table	Displays what servers and storage devices are connected to the SAN.
Zone Administration	Allows you to define alias, zone members, and configurations.
Switch Management Application	Displays switch enclosure information, confirms general switch information, and includes user interface buttons for quick access to the Administrative Interface, Telnet Interface, and Performance.
Performance	Displays real-time data throughput for each port and switch bandwidth utilization.
Port Detail	Displays statistics and general information for all ports, including LED status.
Administrative Interface	Lets you perform management functions such as enabling and disabling ports and upgrading firmware.
Telnet Interface	Lets you use Telnet commands for switch management, diagnostics, and troubleshooting.

User View Pages

TopZoneNS Page

To access the TopZoneNS page, enter the IP address or switch name as the URL in a browser, for example, http://it4 or http://192.168.60.54. You can also launch this page from the SWCC fabric window by selecting the TopZoneNS link or right-clicking on a switch and selecting TopZoneNS.

Use the TopZoneNS page to display all switches in the fabric. This page can show up to 239 switches in a grid and uses IP addresses or switch names to connect to individual switches. Each switch must have a unique name that matches the correct IP address by the name resolution protocol in use by the Web client. If a switch name is not recognized by the name resolution protocol, the switch can be accessed by typing its IP address.

NOTE: The Compaq StorageWorks Fibre Channel SAN Switch software (version 2.0 and above) is compatible with the Compaq StorageWorks Fibre Channel Storage Switch software (Version 1.6b or 1.6d), allowing both types of switches to operate in the same fabric. To accomplish this compatibility, a Fibre Channel SAN Switch must be configured to use a specific addressing mode. This mode is designated "VC Encoded Address Mode."

Invoke this mode using the configure command, as described in Appendix A. When using this compatibility mode, the maximum switch count in a fabric is reduced from 239 to 32, and the maximum number of multicast groups is reduced from 256 to 31.

If the compatibility mode is not set, the following error message displays when you interconnect a Fibre Channel SAN Switch and a Fibre Channel Storage Switch:

FABRIC, SEGMENTED, LOG_WARNING
Description: Fabric segmented.
Probable Cause: Incompatible fabric parameters/switches or conflict zones.
Action: Reconfigure fabric or zones. See configure command.

The TopZoneNS page displays the front panel of each switch and the name, Domain ID, Ethernet IP address, FCnet IP address, Gateway IP address, and World Wide Name. Double-click a switch's image to display the Switch Management Application page for that switch.

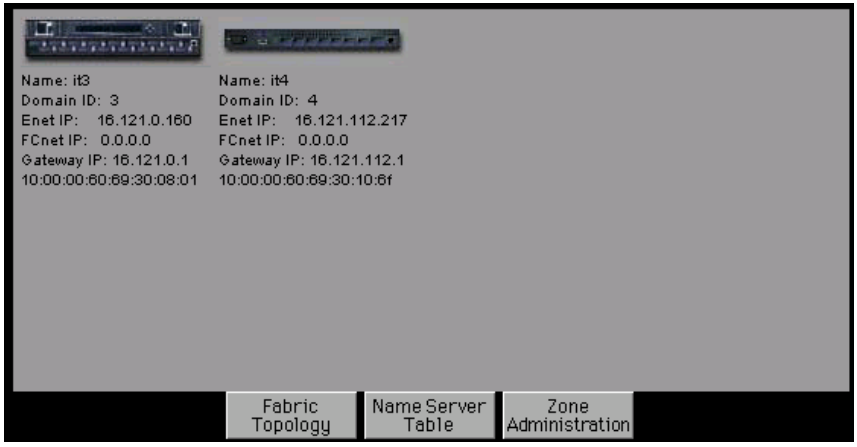


Figure 3-1. TopZoneNS page

Fabric Topology Page

Use the Fabric Topology page to display physical configuration information, including active domains and paths, and routing information.

Figure 3-2 shows the Fabric Topology page. The fabric topology is viewed from the host domain (or host switch) that is initially requested from the Web browser.

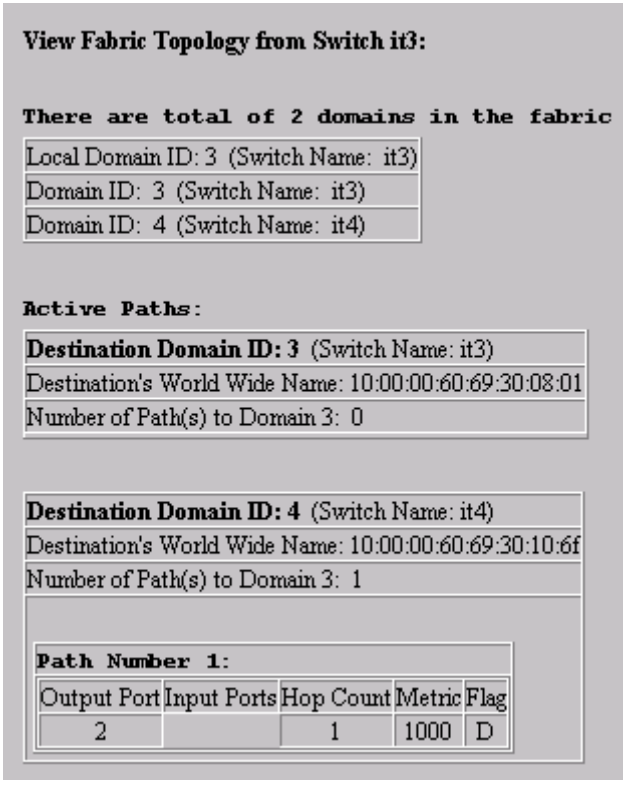


Figure 3-2. Fabric Topology page

Table 3-2 describes the fields on the Fabric Topology page.

Table 3-2
Fabric Topology Fields

Field	Description
Active domains	Displays the number of active domains in the fabric including switch names and switch domain Ids.
Active paths (by domain)	Displays active paths from the local domain to all remote domains in the fabric, and includes the domain ID associated with the switch name, WWN, and total number of paths to the domain. Each path is displayed including: ■ Local switch output port number. ■ Destination switch input port numbers. ■ Hop count – Number of interswitch links that must be transversed to get from source to destination. ■ Metric – cost of using this path. ■ Flag – D = DYNAMIC, S = STATIC

Name Server Table Page

Use the Name Sever Table page to display name server entries for the fabric that are kept in the Simple Name Server database. This includes all name server entries, not just those local to a single switch.

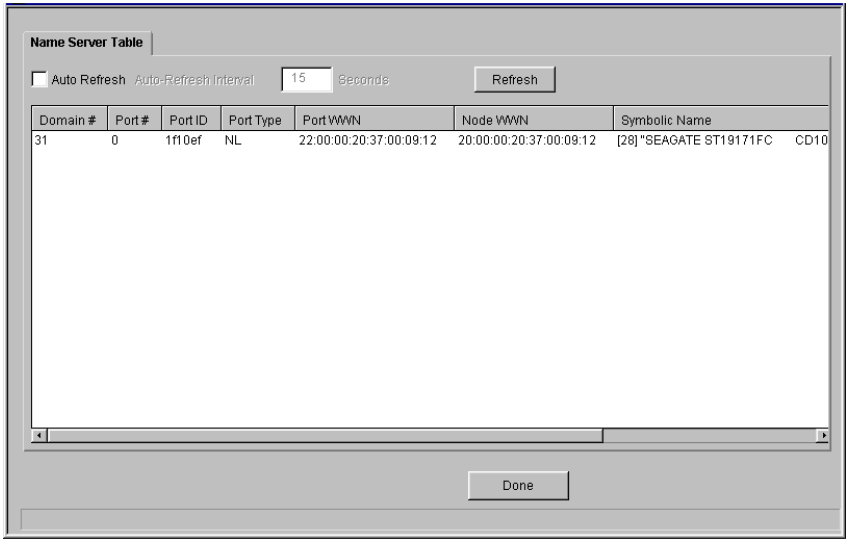


Figure 3-3. Name Server Table page

Table 3-3 describes the fields on the Name Server Table page.

Table 3-3
Name Server Table Fields

Field	Description
Auto Refresh	Click to enable Auto Refresh. Clear to disable.
Auto refresh Interval	Displays refresh interval, in seconds.
Refresh	Click to refresh on demand.
Domain #	Displays switch's domain ID each device is connected to.
Port #	Displays switch's port number each device is connected to.
Port ID	Displays device's port ID (Fibre channel 24-bit ID in hexadecimal).
Port Type	Displays device's port type (N for fabric direct attached port or NL for fabric direct attached loop port).

continued

Table 3-3
Name Server Table Fields *continued*

Field	Description
Port WWN	Displays device port's World Wide Name.
Node WWN	Displays device node's World Wide Name.
Symbolic Name	Displays device's symbolic name assigned through the SCSI INQUIRY command.
FC4 Types	Displays Fibre Channel FC4 layer types supported by device, such as IP, FCP, and so on.
COS	Displays Fibre Channel classes of service supported by the device.
Member of Zones	Lists member zones for this device.

Zone Administration Page

Use the Zone Administration page to configure and manage:

- Zone Alias Settings
- Zone Settings
- Zone Configuration Settings

For detailed information on Zoning see Chapter 6, "Understanding and Using Zoning."

Zone Alias Settings Page

Aliases are easy to remember names used instead of port numbers or worldwide names, for example, Engineeringsvr.

Use the Zone Alias Settings page to configure and manage alias members. (Zone aliases are optional). To access the Zone Alias Settings page, click the Zone Administration button from the TopZoneNS page then click the Zone Alias Settings tab.

To create a zone alias:

1. Choose the Zone Alias Settings tab.
2. Select the Create Alias button and enter a name for the alias (choose a name that is easy to remember).
3. Choose a member from the Member Selection List and select the Add Member > button. Each member is added to the right side under the new alias member's name entered in step 2.

   Repeat this step for each member that you want added to the alias members.
4. Select Apply.
5. Select Done.

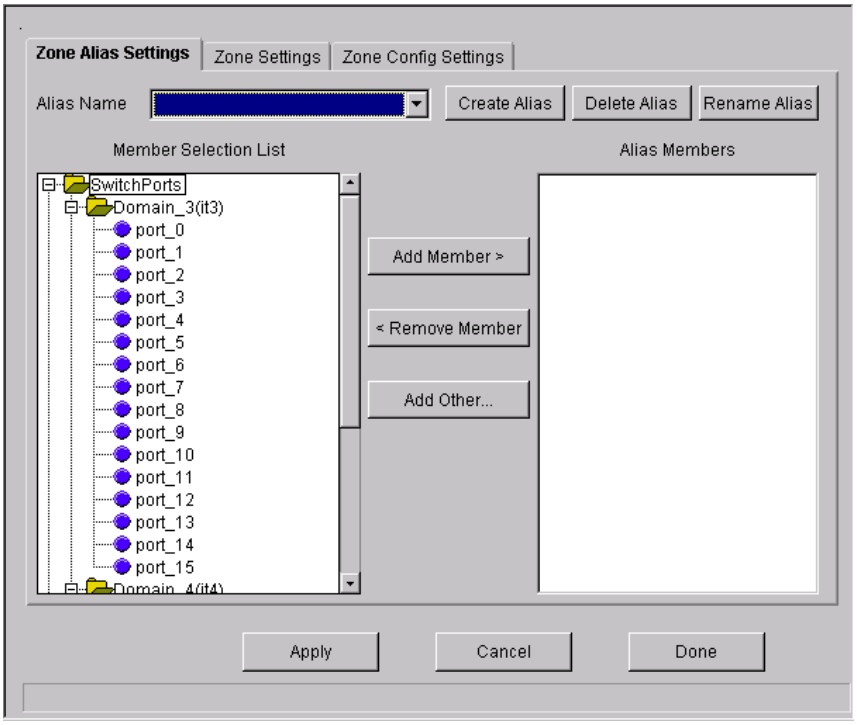


Figure 3-4. Zone Alias Settings page

Table 3-4 describes the fields on the Zone Alias Settings page.

Table 3-4
Zone Alias Settings Fields

Field	Description
Alias Name	Displays currently selected alias.
Create Alias	Enter name of new alias; all names must be unique and should not contain spaces.
Delete Alias	Delete alias appearing in Alias Name field.
Rename Alias	Enter new name for currently selected alias.
Member Selection List	Displays available switches, ports, and WWNs.
Add Member	Select a member from Member Selection List and click Add Member button to add to the list of members for the currently selected alias.
Remove Member	Select a member from list of members for the currently selected alias and click Remove Member button to remove from the member list.
Add Other	Add switch domain, port, WWN not in member selection list.
Alias Members	Displays members of currently selected alias.

Zone Settings Page

Use the Zone Settings page to create, delete or rename zones, or to add or delete members from zones.

To create a zone:

1. Select the Zone Settings tab.
2. Select the Create Zone button and enter a name for the zone.
3. Choose a member from the Member Selection List and select the Add Member > button. The member is added to the right side under the new zone member's name entered in step 2.

   Repeat for each member that you want added to the zone members.
4. Select Apply.
5. Select Done.

Zone Settings can create a special broadcast zone.

To create a broadcast zone:

1. Place all participating devices into a broadcast zone.
2. Place the broadcast zone into a zone configuration.
3. Enable that zone configuration.

To access the Zone Settings page, click the Zone Administration button from the TopZoneNS page then click the Zone Settings tab.

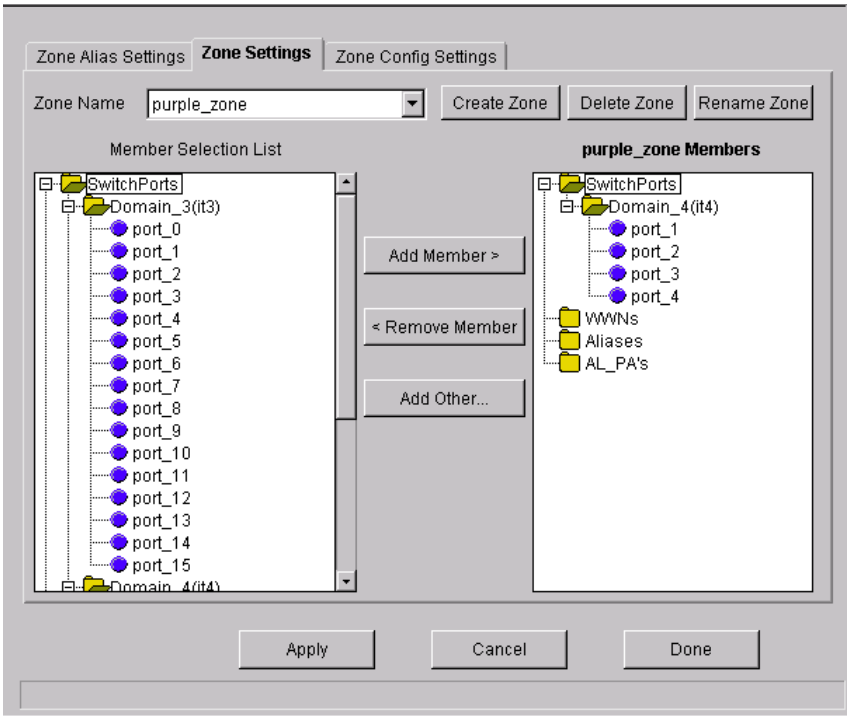


Figure 3-5. Zone Settings page

Table 3-5 describes the fields on the Zone Settings page.

Table 3-5
Zone Settings Fields

Field	Description
Zone Name	Displays currently selected zone.
Create Zone	Enter name of new zone; all names must be unique and should not contain spaces.
Delete Zone	Delete currently selected zone.
Rename Zone	Enter new name for currently selected zone.
Member Selection List	Displays available switches, ports, and WWNs.
Add Member	Select a member from Member Selection List and click Add Member button to add to the list of members for the currently selected zone. If a switch is selected, the switch and all ports are added to the zone. Individual ports are added by selecting a port from within a switch. To add a device WWN, select a node WWN (folder icon) or port WWN (blue circle icon) from the WWN sub-tree. To add an alias, select it from the Aliases sub-tree; zone aliases must have been previously created.
Remove Member	Select a member from list of members for the currently selected zone and click Remove Member button to remove from the member list.
Add Other	Add members that are not in the member selection list. The dialog box prompts for a WWN or Domain, Port.
Zone Members	Displays members of currently selected zone.

Zone Configuration Settings

Use the Zone Configuration Settings page to create zone configurations, place zones into configurations, or to rename or delete zone configurations. To access the Zone Configuration Settings page, click the Zone Administration button from the TopZoneNS page then click the Zone Config Settings tab.

To create a zone configuration:

1. Select the Zone Config Settings tab.
2. Select the Create Cfg button and enter a name for the configuration.
3. Choose a zone from the Zone Selection List and select the Add Member > button. The member is added to the right side under the new configuration zone member's name entered in step 2.

   Repeat for each zone that you want added to the zone configuration name.
4. Select Apply.
5. Select Done.

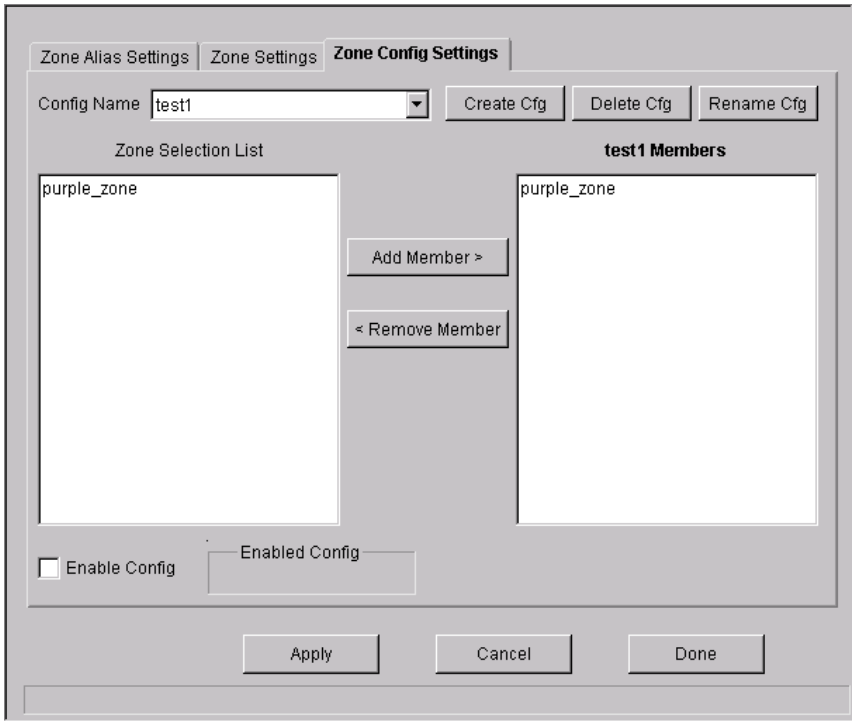


Figure 3-6. Zone Configuration Settings page

Table 3-6 describes the fields on the Zone Configuration Settings page.

Table 3-6
Zone Configuration Settings Fields

Field	Description
Config Name	Displays currently selected configuration name.
Create Config	Enter name of new configuration. All names must be unique and should not contain spaces.
Delete Config	Delete currently selected configuration.
Rename Config	Enter new name for currently selected configuration.
Zone Selection List	Displays available zones that can be added to the selected configuration.

continued

Table 3-6
Zone Configuration Settings Fields *continued*

Field	Description
Add Member	Select a member from Zone Selection List and click Add Member button to add to the list of selected configuration members.
Remove Member	Select a member from list of configuration members and click Remove Member button to remove from the member list.
Config Members	Displays members for the currently selected zone configuration. Only one configuration may be enabled at a time. If none of the configurations are enabled, the zone configurations are not active in the fabric.
Enable Config	Click on to enable the currently selected configuration. Click off to disable.
Enabled Config	Displays the currently enabled configuration.

Switch Management Application Page

To view the Switch Management Application page, double-click on a switch on the TopZoneNS page or by double-clicking the SWCC switch button.

Use the Switch Management Application page to display a graphic representation of the front panel of each connected switch. Normal long-term monitoring is conducted from this page, which provides a real-time view of each switch's overall health and status in the fabric. Switch status is updated every 1 to 2.5 seconds, depending on the operating system and Web browser used.

The upper half of the screen shows port and LED indicator status, while the lower half displays general switch information. Figure 3-7 shows an example of the image that displays for a StorageWorks SAN Switch 8-EL. Table 3-7 summarizes the Switch Management Application page's components.

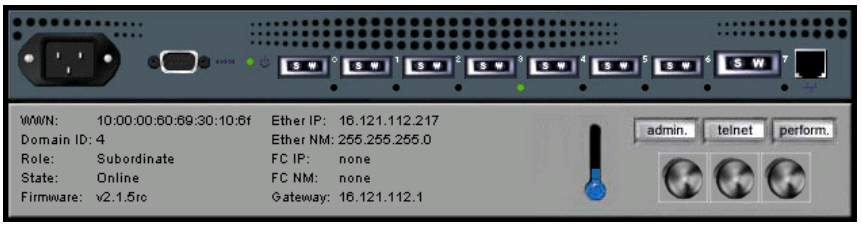


Figure 3-7. Switch Management Application page—StorageWorks SAN Switch 8-EL example

Table 3-7 describes the components in the Switch Management Application page.

Table 3-7
Switch Management Application Fields

Component	Description
Port icons	Link to the Port Detail page.
admin button	Links to the Administration pages.
perform button	Links to the Performance page.
telnet button	Launches a Telnet session.
Thermometer	Indicates the highest temperature from the last data sample. Click the thermometer to display the temperature readings from all switch sensors.
Fans	Indicates the status of the switch's fans.
Power Supplies*	Left and right power assemblies show presence/absence and status of each power supply.
WWN	Lists a unique numeric identifier for each switch.
Domain ID	Displays a number from 0 to 239 that uniquely identifies each switch in a fabric.
Role	Identifies the switch's role: ■ Principal—The switch is the principal switch as defined in FC-SW protocol. ■ Subordinate—The switch is enabled, but it is not the principal switch. ■ Disabled—The switch is disabled.
State	Reports the switch state: Online, Offline, Testing, or Faulty.
Firmware	Lists the firmware version.
EtherIP	Lists the switch's Ethernet IP address.
Ether NM	Lists the Ethernet subnetmask.
FC IP	Lists the Fibre Channel IP address.
FC NM	Lists the Fibre Channel subnetmask.
Gateway	Lists the gateway address.

NOTE: *This functionality is only available on some switch models.

Warning Messages

A warning message automatically displays in a popup window if a problem occurs in the switch. For example, a warning displays if the switch's temperature exceeds maximum value, a fan stops rotating; or if a port state becomes problematic. Use the buttons located at the bottom of the warning message popup window to launch a new browser window that displays basic troubleshooting procedures.

Port Status

Each port icon includes the port number, an LED indicator, and GBIC information. If a GBIC is not present, a silver rectangle is displayed. If the port icon contains a GBIC, one of the following displays:

- "SW" for shortwave fiber GBIC modules
- "LW" for longwave fiber GBIC modules
- "ID" for Serial ID GBIC modules

The color and flash speed of each LED indicator on the switch's front panel show port status. A failed port is outlined in amber on the screen. LED indicator states are defined in the following table.

Table 3-8
Port LED Indicator States

LED Indicators	Definition
No light showing	No light or signal carrier (no GBIC module or cable installed) for media interface LEDs.
Steady amber	Receiving light or signal carrier, but not online yet.
Slow amber	Disabled, flashes every 2 seconds.
Fast amber	Error or fault with port, flashes every half second.
Steady green	Online (connected with device over cable.)
Slow green	Online but cannot make a proper fabric connection (loopback cable installed, fabric is segmented, or switch is connected to an incompatible switch) flashes every 2 seconds.

continued

Table 3-8
Port LED Indicator States *continued*

LED Indicators	Definition
Fast green	Internal loopback (diagnostic), flashes every half second.
Flickering green	The port is active and transferring data and frame traffic.
Alternating green and amber	The port is bypassed.

Port Detail Page

Use the Port Detail page to display statistics for each port. This page has one tab for each port. Clicking on a tab brings the corresponding port window to the front. Each port window displays general port information, such as the port's number, type (E-Port, G-Port, and so on), status, and WWN name, as well as more detailed port statistics.

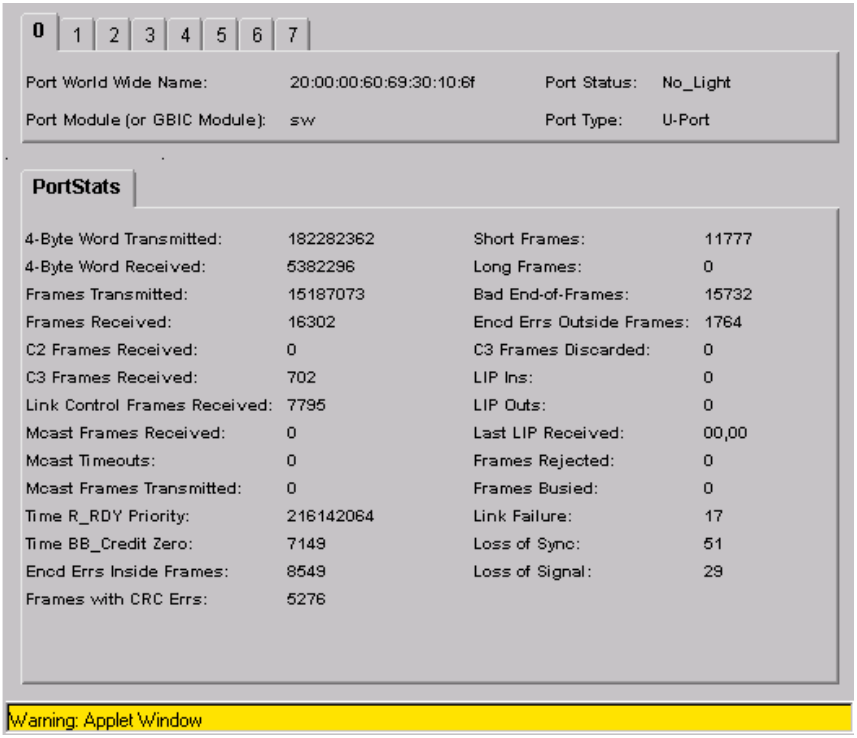


Figure 3-8. Port Detail page

Table 3-9 describes the fields on the Port Detail page.

Table 3-9
Port Detail Fields

Field	Description
Port Number	The port number.
Port World Wide Name	The World Wide Name for this port.
Port Status	The port state follows the GBIC type. The possible port states include: ■ No_Module—No GBIC module in this port. ■ No_Light—The module is not receiving light. ■ No_Sync—The module is receiving light but is out of sync. ■ In_Sync—The module is receiving light and is in sync. ■ Laser_Flt—The module is signaling a laser fault (defective GBIC). ■ Port_Flt—The port has been marked as faulty (defective GBIC, cable, or device). ■ Diag_Flt—The port failed diagnostics. ■ Online—The port is up and running. ■ Lock_Ref—The port is locking to the reference signal.
Port Module (or GBIC Module)	The GBIC type follows the port number. The three GBIC types include: ■ -- —No GBIC present ■ sw—Shortwave GBIC ■ lw—Longwave GBIC ■ id—Could include any of the above.
Port Type	The port type (E_Port, G_Port, U_Port, F_Port, FL_Port, or L-port.)

continued

Table 3-9
Port Detail Fields *continued*

Field	Description
Port Statistics	
4-Byte Word Transmitted	The number of four-byte words transmitted.
4-Byte Word Received	The number of four-byte words received.
Frames Transmitted	The number of frames transmitted.
Frames Received	The number of frames received.
C2 Frames Received	The number of class 2 frames received.
C3 Frames Received	The number of class 3 frames received.
Link Control Frames Received	The number of link control frames received.
Mcast Frames Received	The number of multicast frames received.
Mcast Timeouts	The number of multicast timeouts.
Mcast Frames Transmitted	The number of multicast frames transmitted.
Time R_RDY Priority	The number of times R_RDY has priority over frames to be sent.
Time BB_CreditZero	The number of times BB_Credit went to zero.
Encd Errs Inside Frames	The number of encoding errors inside frames.
Frames with CRC Errs	The number of frames with CRC errors.
Short Frames	The number of frames shorter than minimum.
Long Frames	The number of frames longer than maximum.
Bad End-of-Frames	The number of frames with bad end-of-frames.
Encd Errs Outside Frames	The number of frames with encoding errors outside frames.
C3 Frames Discarded	The number of class 3 frames discarded.
LIP Ins	The number of LIPs received.
LIP Outs	The number of times the loop was initialized by an FL_Port.
Last LIP Received	The last LIP received: AL_PD, AL_PS.
Frames Rejected	The number of F_RJTs sent.
Frames Busied	The number of F_BSYs sent.

continued

Table 3-9
Port Detail Fields *continued*

Field	Description
Link Failure	The number of times NOS received and sent.
Loss of Sync	The number of times a loss of sync occurred.
Loss of Signal	The number of times a loss of signal occurred.

Performance Page

Use the Performance page to display port and switch throughput in bytes per second. Each port is numbered and throughput for the entire switch displays under the individual port readings.

The horizontal axis represents time elapsed. The port throughput graphs hold up to 60 seconds of performance data, and the switch throughput graph holds up to 4 minutes of performance data. The vertical axis in each graph shows throughput (in bytes per second). The graphs are automatically scaled depending on the switch activity.

The total throughput value is the throughput sum for all ports. The throughput number represents the number of bytes received plus the number of bytes transmitted each second. Since the switch also transmits all data it receives, the total throughput for the switch can be stated as one-half of the throughput sum of all ports.

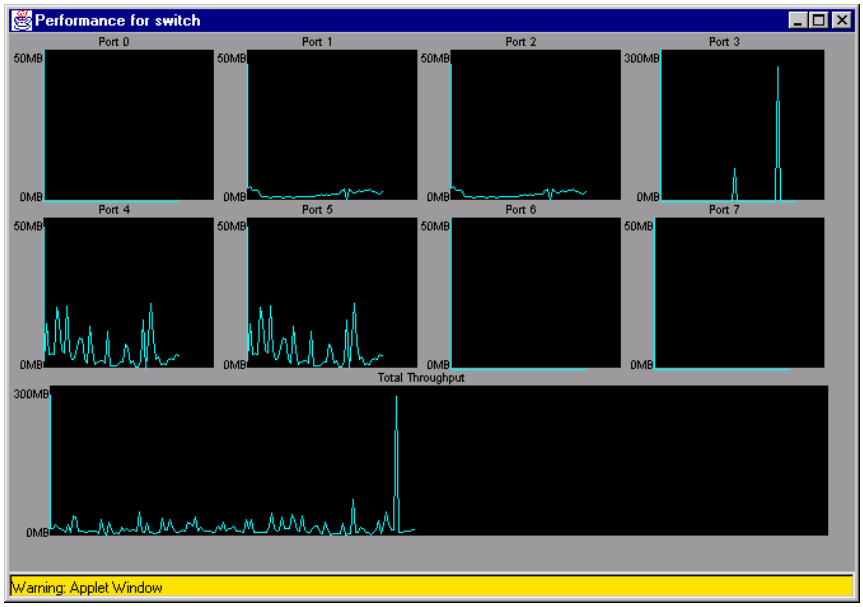


Figure 3-9. Performance page

Administrative Interface Page

The Administrative Interface page contains the following tabs:

- Switch Administration page
- User Administration page
- Firmware Upgrade page
- Reboot Switch page
- SNMP Administration page
- License Administration page
- QuickLoop Administration page
- Remote Switch page (Optional)

To access the Administrative Interface page, click the admin button from Switch Management Application page. To access all other Administration Interface pages, click the appropriate tab for a particular page.

NOTE: You must have administrative privileges to access these pages. See the "User Administration Page," section in this chapter for the default password.

Switch Administration Page

Use the Switch Administration page to change IP information, disable a switch, change the domain, change the switch name, or enable or disable ports.

To access the Switch Administration page, click the admin button from the Switch Management Application page then click on the Switch Admin tab.

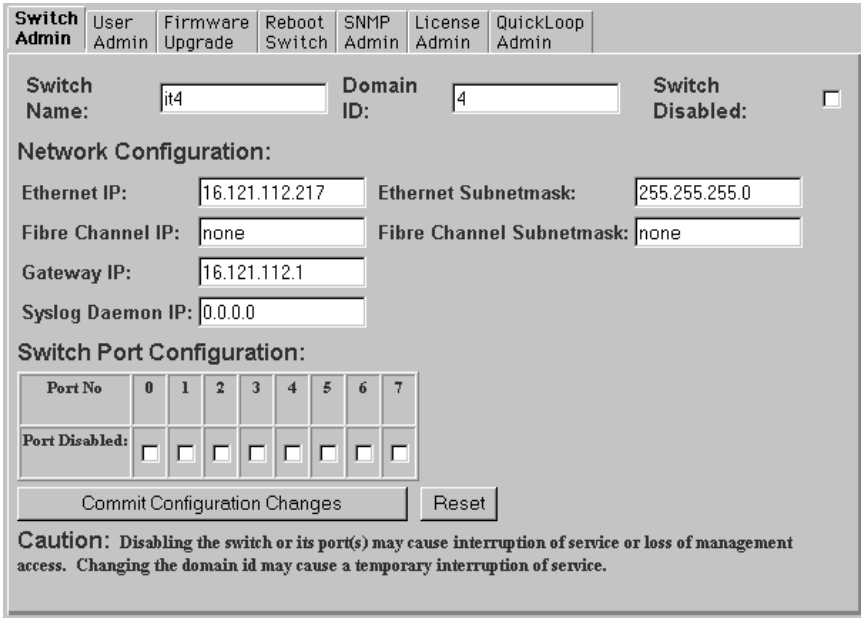


Figure 3-10. Switch Administration page

Table 3-10 describes the fields on the Switch Administration page.

Table 3-10
Switch Administration Fields

Field	Description
Switch Name	Displays or sets the switch name. To change name, enter new name in this field.
Domain ID	Displays or sets switch domain ID. The domain ID must be unique within a fabric. To change domain ID, enter new domain ID in this field. Use a number from 1 to 239 for normal operating mode (FCSW compatible) and a number from 0 to 31 for VC encoded address format mode (backward compatible to Compaq StorageWorks Fibre Channel SAN Switches 8 and 16.)
Switch disabled	Select check box to disable. Clear check box to switch.
Ethernet IP	Displays or sets IP address for Ethernet connection to switch.
Ethernet Subnetmask	Displays or sets Ethernet subnetmask. Default value is none. Contact network administrator for value to enter. If changed, restart browser.
Fibre Channel IP	Displays or sets fibre channel IP address.
Fibre Channel Subnetmask	Displays or sets fibre channel subnetmask. If changed, restart browser.
Gateway IP	Displays or sets gateway IP address. Contact network administrator for IP address. If changed, restart browser.
Syslog Daemon IP	Displays or sets destination station IP address for sending events using syslog protocol to host. Contact network administrator for IP address.
Port Disabled	Select check box to disable port. Clear the check box to enable.

User Administration Page

Use the User Administration page to rename accounts or change passwords.

To access the User Administration page, click the admin button from the Switch Management Application page then click on the User Admin tab.

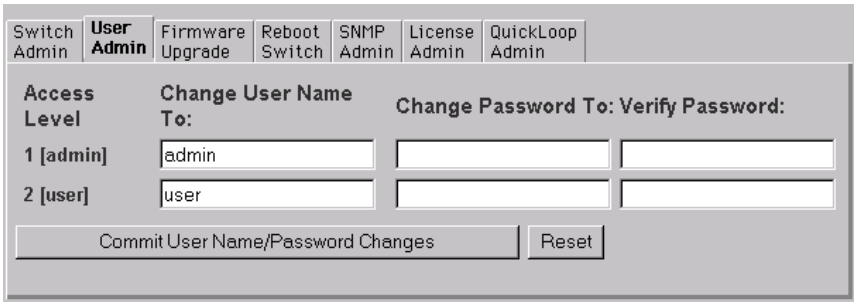


Figure 3-11. User Administration page

Table 3-11 describes the fields on the User Administration page.

Table 3-11
User Administration Fields

Field	Description
Change User Name To	Enter new user name.
Change Password To	Enter new password.
Verify Password	Re-enter password to verify.
Commit User Name/Password Changes	Click to apply changes made.

NOTE: The default password for admin (access level 1) and user (access level 2) is "password". See the "Default Usernames and Security Levels" section in Chapter 4 for more information about the access levels.

Firmware Upgrade Page

Use the Firmware Upgrade page to download firmware upgrades.

To access the Firmware Upgrade page, click the admin button from the Switch Management Application page then click on the Firmware Upgrade tab.

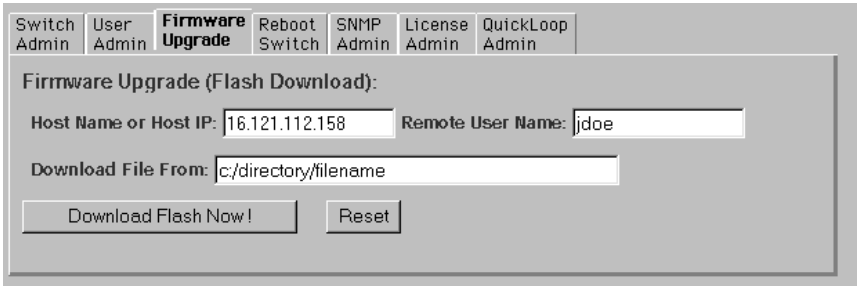


Figure 3-12. Firmware Upgrade page

Table 3-12 describes the fields on the Firmware Upgrade page.

Table 3-12
Firmware Upgrade Fields

Field	Description
Host Name or Host IP	Enter the host computer name.*
Remote User Name	Enter host computer account name.**
Download file from	Displays or sets absolute directory path from source host where binary Fabric Operating System resides. (You must use the UNIX style of forward slash (/) for the path name when downloading the Fabric Operating System from a Windows system.)***
Download Flash Now	Click to download firmware.****

NOTE: *For Windows 9x, Windows 2000, and Windows NT only, enter an IP address.

**For Windows 9x, Windows 2000, and Windows NT only, enter the default name user.

***When the firmware file is located in the same directory as the *Cat.exe* and *Rshd.exe* files, the directory path can be omitted.

****Prior to downloading the firmware, the *Rshd.exe* program must be running from the same directory that contains the *Cat.exe* program or the FTP server must be running.

For more information about the *Rshd.exe* and *Cat.exe* programs, see Chapter 7 "Upgrading Firmware."

NOTE: A switch reboot is required for downloaded firmware code to be executed by the switch.

Reboot Switch Page

Use the Reboot Switch page to reboot or fast boot the switch. Power On Self-Test (POST) can also be disabled for future reboots.

To access the Reboot Switch page, click the admin button from the Switch Management Application page then click the Reboot Switch tab.

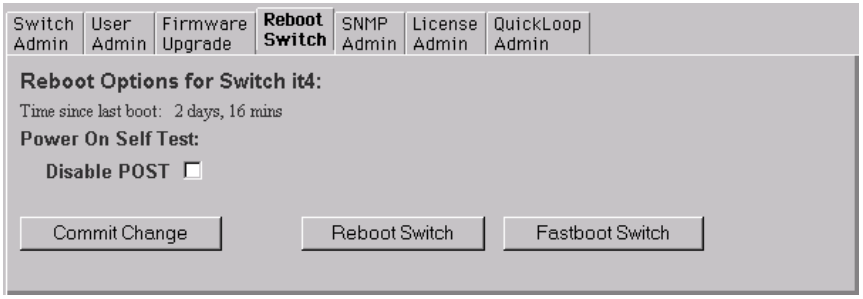


Figure 3-13. Reboot Switch page

Table 3-13 describes the fields on the Reboot Switch page.

Table 3-13
Reboot Switch Fields

Field	Description
Disable POST	Select this check box to disable POST for future reboots. Clear this check box to enable POST.
Commit Change	Click to save settings.
Reboot Switch	Click to reboot the switch.
Fastboot Switch	Click to perform a fast reboot. A fast reboot bypasses POST. (it is the same as a reboot with POST disabled.)

SNMP Administration Page

Use the SNMP Administration page to set SNMP options.

To access SNMP Administration page, click the admin button from the Switch Management Application page then click on the SNMP Admin tab.

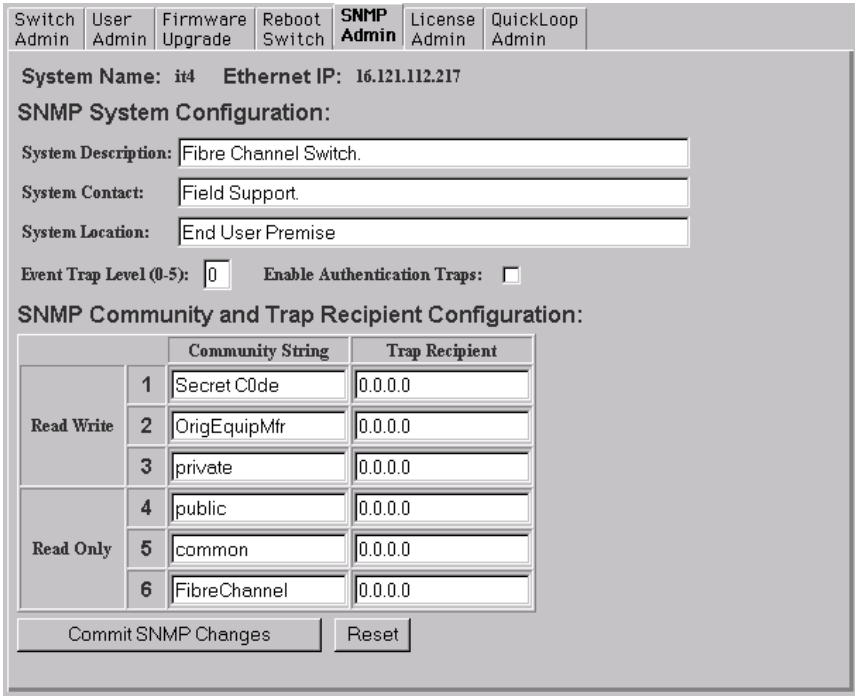


Figure 3-14. SNMP Administration page

Table 3-14 describes the fields on the SNMP Administration page.

Table 3-14
SNMP Administration Fields

Field	Description
System Description	Displays or sets description. Default is Fibre Channel Switch.
System contact	Displays or sets contact information for switch. Default is field Support.
System Location	Displays or sets location of switch. Default is End User Premise.

continued

Table 3-14
SNMP Administration Fields *continued*

Field	Description
Event Trap Level	Sets severity level of switch events that prompt SNMP traps. Default is 3. See the "Agent Configuration" section in Chapter 4.
Enable Authentication Traps	Select check box to enable authentication traps (recommended); clear check box to disable.
Read Write Community String	Displays or sets up to three strings that work with the SNMP set command.
Read Only Community String	Displays or sets up to three strings that work with the SNMP get or get-next command.
Trap Recipients	Displays or sets recipients for traps (usually IP address of SNMP management station).
NOTE: To disable the community string or trap recipients' fields, leave them empty.	

License Administration Page

Use the License Administration page to add or remove licenses. A list of installed license keys and features is also displayed.

To access License Administration page, click the admin button from the Switch Management Application page then click on the License Admin tab.

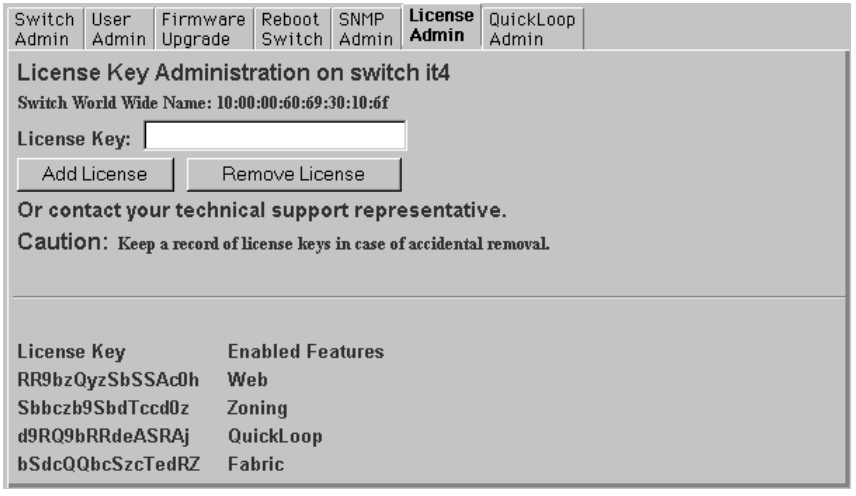


Figure 3-15. License Administration page

Table 3-15 describes the fields on the License Administration page.

Table 3-15
License Administration Fields

Field	Description
License Key	Enter license key to be added or removed.
Add License	Click to add specified license.
Remove License	Click to remove specified license.
Keys and enabled Features	Displays license keys and features enabled on switch.

CAUTION: Once a license is removed, the functionality and the license are disabled. Make sure to write down the license number and keep it in a safe place.

QuickLoop Administration Page

Use the QuickLoop Administration page to set up a QuickLoop for a single switch or for a pair of switches. Select the switches, enable or disable a QuickLoop at the switch level, and turn QuickLoop on or off on an individual port.

NOTE: QuickLoop is not available for the Compaq StorageWorks Fibre Channel SAN Switch 8-EL.

For detailed information on QuickLoop, see Chapter 5, "Overview of the Fabric Operating System and QuickLoop."

To access the QuickLoop Administration page, click the admin button from the Switch Management Application page then click on the QuickLoop Admin tab.

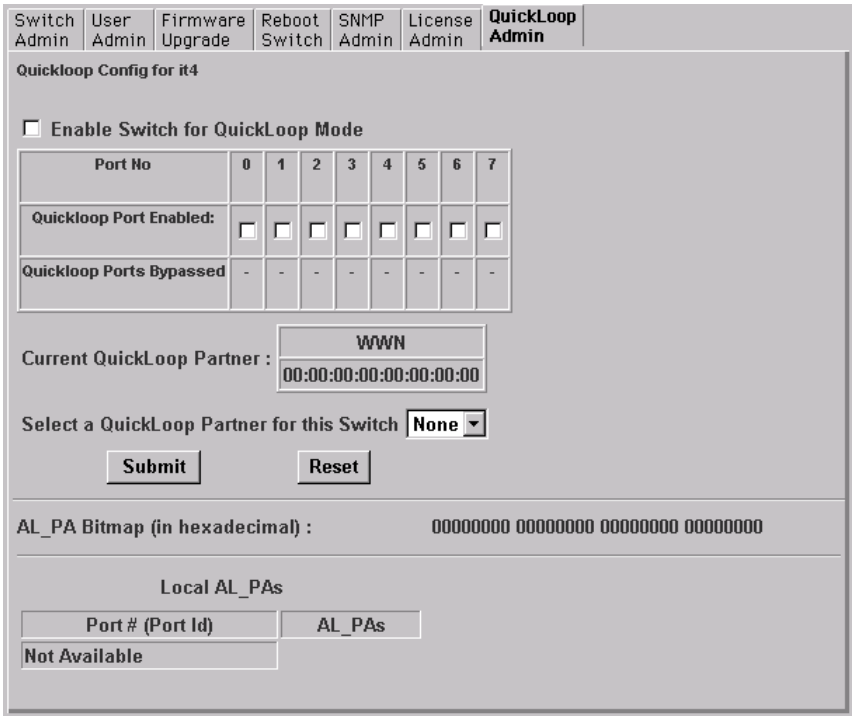


Figure 3-16. QuickLoop Administration page

Table 3-16 describes the fields in the QuickLoop Administration page.

Table 3-16
QuickLoop Administration Fields

Field	Description
Enable Switch for QuickLoop Mode	Select the check box to enable the switch for QuickLoop. Clear the check box to disable the switch for QuickLoop.
Port No	Port Number
QuickLoop Ports Enabled	Select a check box to enable QuickLoop on that port. Clear a check box to disable QuickLoop on that port.
QuickLoop Port Bypassed	If a check box is selected, this indicates a port is currently bypassed.

continued

Table 3-16
QuickLoop Administration Fields *continued*

Field	Description
Current QuickLoop Partner	Displays the current partner switch WWN, domain ID, and switch name of a dual-switch QuickLoop.
Select a QuickLoop Partner for this Switch	Select a switch from the list of switch names currently in the fabric as the partner switch of a dual-switch QuickLoop.
AL_PA Bitmap	Displays the AL_PA bitmap at the end of a QuickLoop initialization.
Local AL_PAs	Lists the AL_PAs of devices connected to the local switch.
Remote AL_PAs	Lists the AL_PAs of devices connected to the remote switch if dual-switch QuickLoop is configured.

Remote Switch Page (Optional Software, License Required)

Use the Remote Switch page to configure a pair of switches to operate over an extended WAN interface so that they can communicate across an ATM network by using a CNT Fibre Channel to ATM interface. This feature requires an active Remote Switch sub-license in both switches.

For detailed information on the Remote Switch, refer to the *Compaq StorageWorks SAN Switch Remote Switch Services Installation Guide.*

To access Remote Switch page, click the admin button from the Switch Management Application page then click on the Remote Switch tab. The Remote Switch tab will only show up on the Switch Management Application page if a remote switch license is installed.

Table 3-17 describes the fields on the Remote Switch page.

Table 3-17
Remote Switch Fields

Field	Description
Remote Switch Enabled	Select the check box to enable the remote switch. Clear the check box to disable the remote switch.
Commit remote Switch	Click to apply changes made.

Telnet Interface Page

The Telnet Interface page lets you launch a Telnet session directly from your Web browser. To launch a Telnet session, click the Telnet button in the Switch Management Application page.

Only one Telnet session can be active at a time. A message box appears if a session is already active. Click ABORT SESSION to terminate the session that is active or click CANCEL to cancel the new session. An up arrow D appears in the Telnet session that is terminated.

NOTE: User and administrative privileges can access this page but only administrative privileges can abort a telnet session.

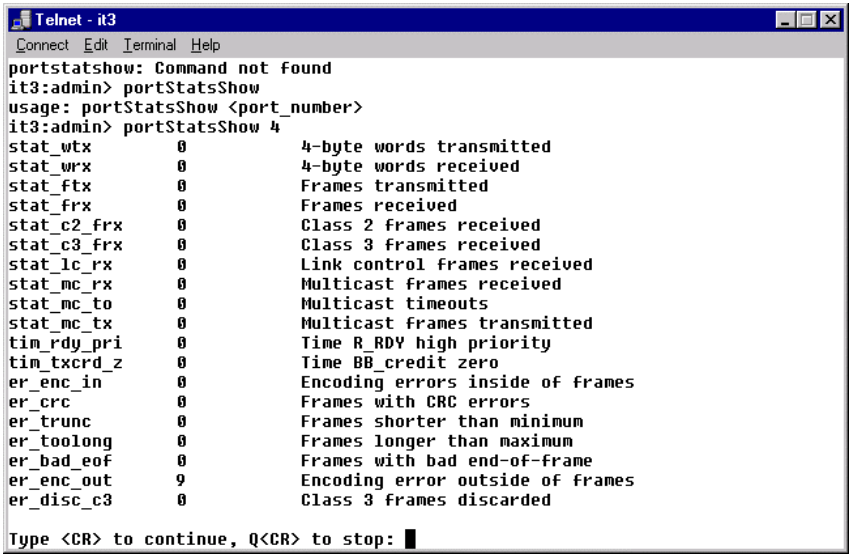


Figure 3-17. Telnet Interface page

See Appendix A for detailed information about Telnet commands.

NOTE: HotJava browsers do not support Telnet commands.

Useful Information

When using Web Management Tools, note the following:

- Fields that can be modified are highlighted.
- Hints display in the bottom left of your browser when you position your mouse over highlighted areas.
- When making changes in the Admin page, the Response Page shows whether each individual configuration change was committed or rejected.
- Java is disabled in some versions of Netscape Navigator and must be enabled by selecting both the Enable Java and the Enable Java Script options in the Preferences/Advanced menu.
- Java applications can hang Netscape Navigator and Microsoft Internet Explorer (IE) on Windows NT after Service Pack 3 due to the True Color graphics-specific mode. To work around this problem, either change the Windows NT display settings to other than True Color, or download Microsoft's hotfix to modify the *Win32k.sys* file. The hotfix is available from Microsoft Technical Support.

Chapter 4

Managing the Switch Using SNMP, Telnet, or Single Ethernet Port

This chapter covers the following topics:

- Managing the switch using SNMP
- Managing the switch using Telnet
- Fabric Management through a single Ethernet port
- Syslog Daemon

Managing the Switch Using SNMP

The switch's resident SNMP agent allows remote switch management through the IP over Ethernet and Fibre Channel interfaces. This section provides an overview of the key concepts in switch management based on SNMP.

SNMP Model

Within the SNMP model, a manageable network consists of one or more manager systems (or network management stations) and a collection of agent systems (or network elements).

- A manager system runs a management application, such as the SWCC, that monitors and controls the network elements.
- An agent system is a network device, such as a Fibre Channel switch, a managed hub, or a bridge, that has an agent responsible for carrying out operations requested by the manager. Therefore, an agent is the interface to a managed device.

The manager communicates with an agent by using SNMP. The switch agent supports SNMP version 1 (SNMPv1) and Community-based SNMP version 2 (SNMPv2C). SNMP allows the following management activities:

- A manager can retrieve management information from an agent. There are three operations for this activity:
  - SNMP-GET
  - SNMP-NEXT
  - SNMP-BULKGET (SNMPv2C)
- A manager can change management information on the agent. This operation is called SNMP-SET.
- An agent can send information to the manager without being explicitly polled for it. This operation is called a trap in SNMPv1 and a notification in SNMPv2C. Traps or notifications alert the manager to events that occur on the agent system. For the rest of this guide, the term *trap* is used.

Management Information Base

The information on an agent is known as the Management Information Base (MIB). It is collection of configuration and status information. A specific type or class of management information is known as a MIB object or MIB variable. For example, the MIB variable sysDescr describes an agent system. The existence of a particular value for a MIB object in the agent system is known as a MIB object instance, or simply an instance. Some MIB objects have only a single instance for a given agent system. For example, the system description and the instance are denoted as sysDescr.0. Other MIB objects have multiple instances. For example, the operational status of each Fibre Channel port on a switch and a particular instance can be denoted as swFCPortOperStatus.5.

MIB objects are organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier. Intermediate branches of the tree serve as a way to group related MIB objects together and the leaves of the tree represent the MIB objects. Figure 4-1 illustrates the tree structure.

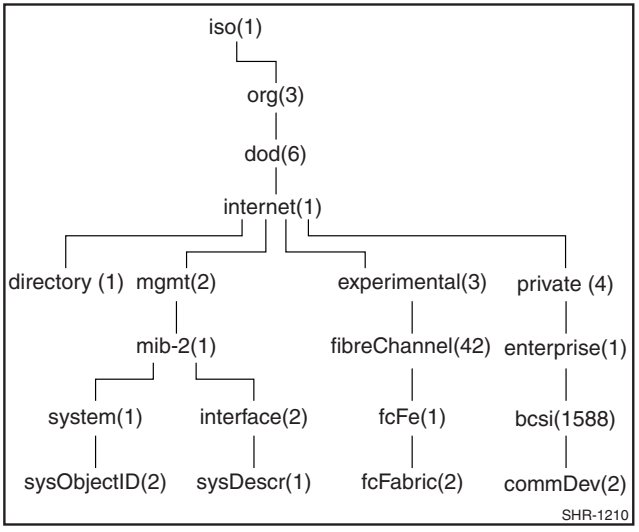


Figure 4-1. Management Information Base (MIB) tree

A MIB object is identified by its position in the tree. A full object identifier consists of the identifier of each branch along the path through the tree. For example, the object sysObjectID has the full identifier of 1.3.6.1.2.1.1.2. For readability, the notation {system 1} can be used.

The switch's agent supports the following:

- SNMPv1 and SNMPv2c
- Command line utilities to provide access to and configuration of the agent
- MIB-II system group, interface group, and SNMP group
- Fabric element MIB
- Vendor-specific MIBs
- Standard generic traps
- Enterprise-specific traps

SNMP Transports

The SNMP agent residing on the embedded processor supports UDP/IP over the Ethernet interface or any FC-IP interface. This transport provides an immediate plug-and-play support for the switch after the IP address has been assigned.

MIB-II Support

Eleven groups of objects are specified in MIB-II. The SAN Switch SNMP agent supports three of these groups. The three supported groups include:

1. System group (object ID is {iso, org, dod, internet, mgmt, mib-2, 1})
2. Interfaces group (object ID is {iso, org, dod, internet, mgmt, mib-2, 2})
3. SNMP group (object ID is {iso, org, dod, internet, mgmt, mib-2, 11})

The following variables can be modified by using the SNMP set command, given an appropriate community with read-write access:

- SysDescr—The system description; the default value is set as Fibre Channel Switch.
- SysObjectID—The system object identifier vendor's authoritative identification (1.3.6.1.4.1.1588.2.1.1.1)
- SysUpTime—The time since the agent was last initialized
- SysContact—The identification and contact information for this system. By default, this is set as Field Support.

- SysLocation—The node's physical location. The default setting is End User Premise.

The interface group supports three interface drivers: software loopback, Ethernet, and Fibre Channel IP.

Fabric Element MIB Support

There are five object groups defined for fabric element MIB support:

- Configuration group
- Operation group
- Error group
- Accounting group
- Capability group

The SNMP agent supports all groups.

Specific MIBs

There are five groups of MIBs defined for fabric support:

- Switch System group
- Fabric group
- SNMP Agent Configuration group
- Fibre Channel Port group
- Name Server group

Generic Traps

Setting up the switch's SNMP connection to an existing managed network lets the network system administrator receive the following generic traps:

- coldStart—Indicates that the agent has reinitialized itself such that the agent's configuration can be altered. This also indicates that the switch has booted.
- linkDown—Indicates an IP interface (Ethernet, loopback, or embedded N_Port) has gone down and is not available.

- linkUp—Indicates an IP interface (Ethernet, loopback, or embedded N_Port) has become available.

  NOTE: The linkUp and linkDown traps are not associated with removing or adding an Ethernet cable. This is strictly a driver indication that the interface is configured, operational, and available, and does not necessarily mean that the physical network cable is affected.

- authenticationFailure—Indicates that the agent received a protocol message that is not properly authenticated. This trap is disabled by default, but it can be enabled with the command agtcfgSet.

Enterprise-Specific Traps

The fabric supports three enterprise-specific traps. They are:

- swFault—Indicates that the diagnostics detected a fault in the switch.
- swSensorScn—Indicates that the operational state in an environment sensor, such as a fan, the temperature, or a power supply has changed.
- swFCPortScn—Indicates that the operational state in a Fibre Channel port has changed.

  NOTE: SNMP swFCPortScn traps are generated whenever a GBIC is inserted and removed, even though the state remains offline.

- swEventTrap—Indicates a firmware event has been written to the switch event log.

Trap parameters can be configured with the SNMPv1 SET command with an appropriate community. These parameters can also be configured through a Telnet connection with the agtcfgSet command.

Agent Configuration

The agent parameters that can be configured include:

- SNMPv1 communities (up to six)
- Trap recipients (one per community)

  NOTE: You must reboot the switch for changes in the SNMPv1 communities or trap recipient parameters to take effect.

- sysName
- sysContact
- sysLocation

  NOTE: The sysName, sysContact, and sysLocation parameters can be configured by the SNMPv1 SET command with an appropriate community. These parameters can also be configured using a Telnet connection and the agtcfgSet command.

- authenticationFailure
- swTrapEnable
- swEventTrapLevel

  The swEventTrapLevel parameter is a trap that specifies the severity level in conjunction with the security level of an event. When an event occurs, and if its severity level is at or below the set value, the trap is sent to configured recipients. For example, if the trap value is set to 3 (warnings), traps will be sent for 3, 2 (errors), and 1 (criticals). By default, the event trap value is 3.

  Possible trap values include:

  - 0—None
  - 1—Critical
  - 2—Error
  - 3—Warning
  - 4—Informational
  - 5—Debug

- authTrapsEnabled: (true, t, false, f) By default, the parameter is set to t.
- SNMP community and trap recipients configuration:

  These parameters contain the IP address of the trap recipients that have been configured to process the traps. The SWCC Agent will write this address during setup.

These parameters can be changed through SNMP or through Telnet with the agtcfgSet command.

NOTE: Changes to SNMP parameters are not displayed in SNMP until the switch is rebooted. This is because SNMP runs from cache while the active settings run from the flash ROM.

Tools for Managing with SNMP

The SWCC software provides an easy way to set up and manage the switch. The SNMP MIBs are integrated into the SWCC software. Refer to the *Compaq StorageWorks Command Console (SWCC) for Hubs, Switches, and Tape Controllers* documentation included on the software CD for more information.

You can set up trap definitions with a number of tools, including SWCC, Compaq Insight Manager, HP OpenView, and others. To use a tool other than the SWCC, refer to the documentation provided with the tool.

Compaq CNMS SNMP Setup

Complete the following steps to incorporate the Fibre Channel standard MIB and the Compaq-specific MIB into an SNMP management station:

1. Install Compaq-CNMS on your computer.
2. Log in to your computer.
3. Double-click the Compaq-CNMS icon.

When the User Settings wizard displays:

1. Choose Normal and click Next.
2. Choose Default Polling and click Next.
3. Change the default (write) community string to private and click Next.
4. Leave the email choices at their default values and click Next.
5. Leave the Web choices at their default values and click Next.
6. Leave the wizard choices at their default values and click Next.
7. Choose Yes for “manageable devices automatically discovered” and click Next.
8. Enter the gateway router IP address (provided by your network administrator).
9. Leave the “other community strings for read” at their default values and click Next.
10. Leave the “automatic layout settings” at their default values and click Next.

11. At the next window, click Begin Discovery Now. This completes the User Settings wizard entries.

To configure the system for the switch:

1. Go to the Tools pull-down menu and click Create Custom Device. You will be prompted for a Device Type Name.
2. Enter a name, such as "FC Switch," and click Next. You will be prompted for an icon.
3. Click none selected, choose an icon, and click Next.
4. Skip the batch file prompt. You will be prompted for the type of MIB this device supports.
5. From the list, select RFC1213-MIB and click Next.
6. The next window asks you for the SysObject ID. This is the string of numbers that defines the object ID for SNMP. Enter 1.3.6.1.4.1.1588.2.1.1.1 and click Next.
7. The next window prompts for a Physical Port. Enter a name for the Ethernet port, such as "Ethernet Mgmt Port." Click Add Port and choose Ethernet as the protocol.
8. At the next window, click Finish. A message displays stating that you successfully created a custom device type. Exit the program and restart Compaq CNMS for the device type to take effect.
9. When the program starts, the User Settings wizard displays. Click Cancel. The FC Switch icon displays in the networking devices area. This is the custom device type you created.
10. Drag the icon with your mouse and drop it into the window labeled Main. A picture of the FC Switch displays in the Main window.
11. A description of the switch displays. Enter a name and the IP address for your switch. Click OK.
12. Place the cursor on the switch and click the right mouse button. From the menu, choose SNMP Statistics, then System Information. A new window displays the information about the switch as configured through the Telnet command agtCfgSet. The values that display are the default settings. Change them if necessary. After you change the values, verify they are set on the switch through Telnet using the agtcfgShow command or through SNMP.
13. Go back to the SNMP Statistics window and choose Protocols for a list of supported protocols.

14. Go back to statistics and choose MIB Browser. A window displays with three items in a tree. Choose Parse MIBS.
15. Click OK, then choose Browse MIB to parse from the next window.
16. Choose *sw.mib* to compile the MIB. Exit the Parse MIB window, then exit the MIB Browser window.

NOTE: swTrapEnable must be set to 1 and swEventTrap level must be set correctly.

Managing the Switch Using Telnet

To make a successful Telnet connection to a switch, you need the switch name or IP address, a username, a password, and an Ethernet connection

NOTE: The switch must have an IP address. To assign an IP address, refer to the installation and hardware guide that came with your switch.

Default Usernames and Security Levels

Each username has an associated security level, with username 3 having the least number of privileges and username 1 having the most.

Table 4-1
Default Usernames

Default Username	Description
User (username 3)	Gives users access to commands that do not change a switch state. This level is recommended for monitoring switch activity.
Admin (username 2)	Gives users access to all commands in the Help menu. Most switch administration is performed at this level.
Root (username 1)	Gives users access to an extensive command set that can significantly alter system performance. Root commands are beyond the scope of this manual. Consult Compaq customer service before using root commands.

The system administrator can assign usernames other than those listed; however, users at the same security level have the same privileges regardless of the username assigned.

CAUTION: Limit root access to users responsible for maintaining and modifying the fabric. Commands available to a root user, if used inappropriately, can cause the switch to stop functioning or to function abnormally. Root commands should only be used at the request of Compaq customer service.

Changing Passwords

The initial default password for all usernames is password. To change user passwords:

1. Log in as admin.
2. Issue the Telnet command passwd.

   Each username (admin and user) is displayed in sequence, letting you modify each password and name.
3. To replace the existing password, enter a new password or name.

Initiating a Telnet Session

A Telnet session is initiated between a workstation and a switch through an Ethernet connection by establishing a network connection between the host system and the switch's Ethernet RJ-45 connector.

To initiate a Telnet session:

1. Launch Telnet from a workstation connected to the network.

   NOTE: For Windows 95/Windows 98/ Windows NT, select Run from the Start menu. Type Telnet, then click OK.
2. From Telnet, connect to the switch using the switch's IP address.

   NOTE: For Windows 95/Windows 98/ Windows NT, select Remote System from the Connect menu on the Telnet window. Enter the IP address of the switch in the Host Name box.
3. Press **Enter** to display the login prompt. At the prompt, enter admin.
4. At the password prompt, enter the password.
5. When the prompt switchName:userName> displays, enter a Telnet command.

Telnet Commands

Information and examples on managing and monitoring the switch through Telnet are provided in Appendix A of this guide. The following command types are covered:

- QuickLoop-specific commands
- Fabric Operating System and Quickloop commands:
  - **General commands** let you control basic switch operations.
  - **Diagnosis commands** let you monitor, test, and evaluate the switch.
  - **Routing commands** let you view switch routing information.
  - **License commands** let you view, add, and remove license keys.
- Zoning-specific commands

Fabric Management through a Single Ethernet Port

Multiple StorageWorks Fibre Channel switches can be managed through a single IP connection to one of the switches using Telnet services, Web Management Tools, or SNMP commands. Each switch supports a 10BaseT or 10/100BaseT Ethernet connection, which is the general link for IP services. A second IP connection, the Fibre Channel IP or in-band support, is also available for managing a switch.

Most host bus adapters are not set up to initiate an in-band Fibre Channel IP connection. At least one switch must have an Ethernet connection. From that entry point you can manage the remaining switches in the fabric using in-band IP services. The management workstation runs a Web browser, a Telnet session, or SNMP to address the switch that has an Ethernet connection. Therefore, the management workstation and the Ethernet IP address of the switch must be in the same subnet. In addition, the management station must have either a static route to the Fibre Channel IP subnet, or the switch must be the default gateway for the management workstation. This allows the management station to direct IP to or through the switch.

The switches not connected to the Ethernet connection must have:

- The same default gateway value as the switch that is connected to the Ethernet connection.
- FC IP addresses in a different subnet from the Ethernet IP addresses of the management station.
- FC IP addresses in the same subnet as the FC IP address of the switch that is connected to the Ethernet connection.

An Example of Managing the Fabric through a Single Ethernet Port

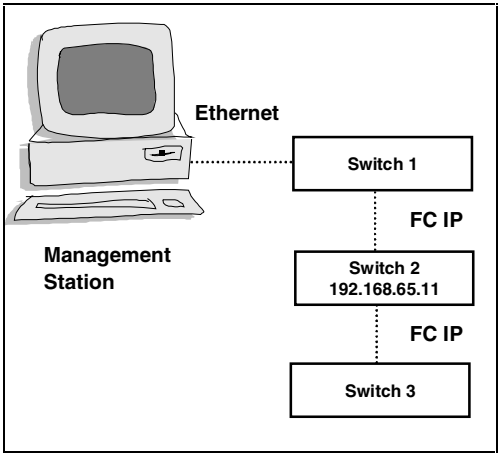


Figure 4-2. Single-port management of switches

To access switch 2 from a browser on the management station, you must enter: http://192.168.65.11

The management station detects that the address is not on the same subnet as the management station so it forwards it to its gateway address (IP address of switch 1). Switch 1 forwards it to switch 2 over the fibre channel.

In the opposite direction, switch 2 detects that the address where the web pages are to be sent are not on the same subnet as switch 2 so it sends the pages to its gateway address, FC IP address of switch 1 which forwards them to the management station.

Table 4-2
Example IP Address Settings

	Management Station	Switch 1	Switch 2	Switch 3
Ethernet IP Address	192.168.1.09	192.168.1.10	204.1.1.11 NC	204.1.1.12 NC
FC IP Address	192.168.65.09	192.168.65.10	192.168.65.11	192.168.65.12
Default Gateway	192.168.1.10	any	192.168.65.10	192.168.65.10

NOTE: Not Connected (NC)

Syslog Daemon

A UNIX-style syslog daemon (syslogd) reads system events, forwards system messages to users, and writes the events to log files according to your system configuration.

Introduction

Syslogd categorizes events by facility and severity. Refer to the manual pages on your UNIX system for a list of facilities and severity levels.

The log process documents errors and system events on the local machine and sends the information to a user or system administrator. The daemon is constantly running and ready to receive messages from system processes. The events are logged according to the statements in the configuration file.

In addition, syslogd can receive messages from a remote machine. Syslogd listens to UDP port 514 for system events. A remote machine does not have to be running UNIX to forward messages to syslogd, but it must follow the basic syslog message format standard.

An example entry in a syslogd log file is:

```
Jul 18 12:48:00  sendmail[9558]: NOQUEUE: SYSERR(uucp):
/etc/mail/sendmail.cf: line 0: cannot open: No such file or directory
```

The first two items are the event's date and time (as known by the machine on which syslogd is running) and the name of the machine that issued the error. This would be the local machine if the message is generated by a task running on the same machine as syslogd, or a remote machine if the message was received on UDP port 514. The first two items are always present while other entries are message-specific.

> **NOTE:** The log file can be located on a different machine and remotely mounted. A local error is an error that occurs where syslogd is running, not on the machine where the error log physically resides.

Syslogd applications for Windows NT and Windows 95 are available at no charge on several FTP servers on the Internet.

Syslogd Support

Switch firmware maintains an internal log of all error messages. The log is implemented as a circular buffer with a storage capability of 30 errors. After 30 errors have been logged, the next error message overwrites the oldest message at the beginning of the buffer.

The switch can be configured to send internal error messages to syslog by sending a UDP packet to port 514 on the syslogd machine. This allows storage of switch errors on a syslogd-capable machine and avoids the limitations of the circular buffer.

Syslogd provides system error support by means of a single log file and can notify a system administrator in real time of error events. The daemon also provides dial home capability.

Error Message Format

Each logged error message sends the following information:

- Error number (1 for the first error after boot, incremented by one with each new error)
- The error message, exactly as it is stored in the error log (and printed by the `errShow` command)

The error number helps identify the error and determine when a switch rebooted. For example, if a log of error number `N` from the switch is followed by a log of error number `0`, then the switch rebooted between the two errors.

The error message includes the switch that reported the error and the following event information:

- ID of the task that generated the error
- Name of the task that generated the error
- Date and time when the error occurred, as seen by the switch. This can be different from the first item in the log file, which is the time of the error as seen by the syslogd machine. These two time values are different if the clocks in the switch and in the syslogd machine are not in sync.
- Error identifier consisting of a module name, a dash, and an error name
- Error severity
- Optional informational part
- Optional stack trace

Example:

Syslogd running on switch sw9 is sending log events to the UNIX machine called example. The following is an example of a no memory error generated by the shell. This is a severity 1 (LOG_CRITICAL) error. Syslogd is configured to store the errors in the */var/adm/silkworm* file similar to the following.

```
example% egrep sw9 /var/adm/silkworm
Jul 11 16:48:25 sw9 1 0x103d8620 (tShell): Jul 11 16:48:19
        Jul 11 16:48:25 sw9Error SYS-NOMEM, 1, No memory
        Jul 11 16:48:25 sw9 Traceback:
        Jul 11 16:48:25 sw9 _tl+0x40 (0x103a2030)
        Jul 11 16:48:25 sw9 _yystart+0x95c (0x1017128c)
        Jul 11 16:48:25 sw9 _yyparse+0x694 (0x10172dc4)
        Jul 11 16:48:25 sw9 _execute+0xdc (0x1014c06c)
        Jul 11 16:48:25 sw9 _shellTask+0x964 (0x1003aea4)
        Jul 11 16:48:25 sw9 _shellTask+0x198 (0x1003a6d8)
        Jul 11 16:48:25 sw9 _vxTaskEntry+0x10 (0x10114d14)
        Jul 11 16:48:25 sw9
```

Message Classification

Syslogd messages are classified according to facility and priority (severity code), which lets a system administrator take different actions for different errors. The action taken, based on the message's facility and priority, is defined in the syslog configuration file. Example configurations are provided in a following section.

The switch uses the facility local7 for all error messages sent to the syslogd.

UNIX provides eight priorities and the switch provides four severity codes [code LOG_PANIC (0) causes a reboot and is not sent to the syslogd]. The mapping between the switch's severity codes and UNIX syslogd priorities is provided in the following table.

Table 4-3
Syslog Message Classification

Switch	UNIX
LOG_CRITICAL (1)	Alert
LOG_ERROR (2)	Err
LOG_WARNING (3)	Warning
LOG_DEBUG (4)	Debug

Switch Configuration

To start the syslogd, type the following command:

```
syslogdIp <IP address of the syslogd machine>
```

The syslogdIp command with no parameter prints the IP address of the current target syslogd machine. An IP address of 0.0.0.0 disables the forwarding of error messages to syslogd. In this case, error messages are logged internally to the switch, but the messages are not forwarded to the syslogd.

Examples

Enable and verify syslogd support:

```
syslogdIp "10.0.0.1"
syslogdIp
syslog daemon's address: 10.0.0.1
```

Disable syslogd support:

```
syslogdIp "0.0.0.0"
syslogdIp
syslog daemon's address: 0.0.0.0
```

Syslogd Configuration

The syslog configuration provides the syslogd with instructions for handling different messages. The following are example entries in a syslog configuration file (*/etc/syslog.conf*) that show the switch error messages that are stored in different files. Refer to the syslog manual pages on your UNIX system for the full documentation of the syslog configuration file. The following entry in */etc/syslog.conf* causes all messages from the switch of UNIX that have a priority warning or higher (switch severity LOG_WARNING or higher) to be stored in the file */var/adm/silkworm*.

```
local7.warning          /var/adm/silkworm
```

The following entries in the */etc/syslog.conf* cause the messages from the switch of UNIX priority alert (switch severity LOG_CRITICAL) to be stored in the file */var/adm/alert*, and all other messages from the switch to be stored in the file */var/adm/silkworm*.

```
local7.alert            /var/adm/alert
local7.debug            /var/adm/silkworm
```

The local7 prefix identifies the switch the message is from. A file must exist and have the proper permission in order for the syslogd to write to it.

Chapter 5

Overview of the Fabric Operating System and QuickLoop

This chapter covers the following topics:

- Overview of the Fabric Operating System
- Overview of the SAN Switch QuickLoop
  - Benefits and features
  - Initialization
  - QuickLoop Master
  - Address translation
  - Operation modes
  - Configurations
  - Fault isolation
  - Recovery
  - QuickLoop Zoning

Overview of the Fabric Operating System

The Fabric Operating System provides a set of services for managing data traffic among SAN devices. The Fabric Operating System includes a complete set of standard Fibre Channel services for fabric and Fibre Channel Arbitrated Loop (FC-AL) management. Sophisticated routing protocols enable you to construct fabrics interconnecting thousands of devices and management services.

The Fabric Operating System lets you:

- Discover the set of connected devices
- Determine the available data paths through the switches
- Configure the fabric automatically
- Configure and manage fabric-wide services such as the Simple Name Service, Alias Service, and Zoning
- Manage the switch remotely using Telnet, SNMP, or Web Management Tools

Features

Table 5-1 describes the software features of the Fabric Operating System.

Table 5-1
Fabric Operating System Features

Feature	Description
Login (FC)	Explicit fabric login is supported (public and private).
Probing	Devices are automatically discovered and registered with the fabric Simple Name Service (SNS). Translation mode is set so private devices can communicate with other fabric attached devices.
Zoning	Zoning is a fabric management service used to create logical device subsets within a SAN, which enables resource partitioning for management and access control.
Buffer-to-buffer credit	The buffer-to-buffer credit for each F_Port can be up to 16 credits.
Time out values	Time out values are adjustable in one-second increments through Telnet. Time out values include R_A_TOVs (Resource Allocation Time Out Values) and E_D_TOVs (Error Detect Time Out Values).

continued

Table 5-1
Fabric Operating System Features *continued*

Feature	Description
Fabric name	Fabric names are automatically or manually assigned for a multiswitch configuration.
Frame delivery	Frames are delivered through the destination F_Port in the same order received by the source F_Port. The in-order frame delivery is maintained within a fabric of multiple interconnected switches.
Address assignment	The switch follows the addressing hierarchy defined in the Fibre Channel Standard. The switch port address identifiers are selected using an automatic address assignment protocol. All ports within the switching fabric (F_Ports, FL_Ports and E_Ports) are assigned address identifiers. Each switch maintains its own address pool. The designated address managers within the fabric manage the address identifiers and assign the address pool to the individual switches.
Broadcast and multicast	The system supports up to 256 multicast groups, plus one for broadcast. Any port can be a member of multiple groups. In addition to the unicast routing table, each port has its own multicast routing table. The Alias Server is responsible for setting up and removing multicast groups.
Frame routing	The system supports self-routing of frames between the communicating ports. The path selection in a multiswitch configuration is based on a self-routing protocol.
Management	The Compaq StorageWorks Fibre Channel SAN Switch 16 can be managed from the front panel controls. The switches can also be managed using SNMP, Web Management Tools, and Telnet. The last three management methods are accessible through the Internet Protocol over the RJ-45 100BaseT Ethernet port or any Fibre Channel port. You can use any SNMP-based management product, including Compaq SWCC, to access the SNMP agent. You can use any supported Web browser to use Web Management Tools.

continued

Table 5-1
Fabric Operating System Features *continued*

Feature	Description
Name Server	The Name Server function is based on the Simple Name Server model defined in the Fibre Channel Standard. The Name Server provides a means to determine which N_Ports are allowed to communicate with each other. This function is provided by the embedded N_Port with the alias address FFFFFCh to register address mapping between the Nx_Port 24-bit Fibre Channel physical address (Nx_Port identifier) and the logical addresses such as World Wide Names (WWNs), IP addresses, FC-4 device types, and Initial Process Associators. The Name Server also provides deregistration and query functions from other nodes or Nx_Ports for logical address translations to the corresponding Nx_Port identifiers.
Alias Server	The Alias Server is based on the Fibre Channel Standard. The function is provided by the embedded N_Port with the alias address FFFFF8h. The server manages multicast groups.

Overview of the SAN Switch QuickLoop

The SAN Switch QuickLoop is a unique Fibre Channel topology that combines the services of fabric and Fibre Channel Arbitrated Loop (FC-AL) management. QuickLoop allows hosts with non-fabric-aware drivers to perform I/O operations with storage devices within a loop.

QuickLoop is a logical Private Loop Fabric Attach (PLFA) consisting of multiple private Arbitrated Loops (looplets) interconnected by a fabric. Although NL_Port devices are attached to different Arbitrated Loops, the fabric and the physical device locations are transparent. All NL_Ports share one Arbitrated Loop Physical Address (AL_PA) space and operate in accordance with the FC-AL.

QuickLoop allows you to use switches instead of hubs in environments where all attached devices are private. No fabric login (FLOGI) is required from these devices. Host drivers that have Private Loop Direct Attach (PLDA) capability do not need to be modified to perform I/O operations with storage devices in QuickLoop.

QuickLoop allows a logical loop of up to two switches if the switches have Fabric Operating System licenses installed. The loop can include all or a subset of the U_Ports in a switch. QuickLoop can be part of a large fabric, and multiple QuickLoops (either single-switch or dual-switch) can coexist in a single fabric.

QuickLoop makes the fabric and the physical connectivity transparent to the NL_Ports by allowing them to communicate with one another using AL_PAs for device addressing. The NL_Ports operate in the same manner as in a PLDA environment. QuickLoop creates a single logical loop that provides a reliable connection between private hosts and storage devices connected to multiple U_Ports (looplets). Loop initializations are propagated to all looplets while detected faults are isolated to a local looplet.

NOTE: This feature is not available on the Compaq StorageWorks Fibre Channel SAN Switch 8-EL.

Benefits

QuickLoop provides a migration path from a single private loop to a fully scalable fabric for constructing SANs. QuickLoop-enabled switches can replace hubs when a SAN is first deployed. When Nx_Port devices become fabric capable, you can upgrade the SAN to mix QuickLoop and fabric, and continue to expand toward a full fabric.

As an alternative to using Fibre Channel hubs, QuickLoop offers many advantages due to the blending of private arbitrated loops and a fabric. These advantages include:

- **More aggregated bandwidth**—Each looplet has its own unshared bandwidth.
- **Higher performance**—Loop tenancies can occur in parallel in different looplets.
- **Better fault isolation**—A looplet, containing a faulty device, is localized.

Features

The SAN Switch QuickLoop:

- Consists of any set of ports from any two switches in a fabric
- Supports a dual-switch configuration for two switches with Fabric Operating System licenses installed
- Supports up to 126 devices per QuickLoop
- Conforms to Fibre Channel standards
- Combines up to 32 ports (Compaq StorageWorks Fibre Channel SAN Switch 16) or 16 ports (Compaq StorageWorks Fibre Channel SAN Switch 8). Each loop attached to a port is referred to as a looplet.

Additional features include:

- Each looplet supports transfer rates of 100 MB/s. Multiple devices can communicate simultaneously in different looplets.
- A fabric can have several QuickLoops, but a switch can only be in one QuickLoop.
- Devices on the QuickLoop are logically attached to the fabric. The first 32 devices are entered into the Name Service and the device address is translated from a 24-bit fabric address to an 8-bit private address.
- Public hosts that support an arbitrated loop attached to QuickLoop ports are treated as private devices.
- Hosts attached to QuickLoop can communicate to all devices attached to QuickLoop.
- Other public hosts connected to the fabric through non-QuickLoop ports can communicate with devices attached to QuickLoop by using single translative mode.
- Individual looplets can be taken out of service manually or automatically if a looplet error is detected. The looplet is reinstated when the error condition is cleared.
- Individual QuickLoop ports can be converted to Fabric Loop Attach (FLA) compliant FL_Ports on switches with a Fabric Operating System license by disabling QuickLoop mode on that port.
- Web Management Tools or Telnet interface can be used for QuickLoop port management.

Initialization

QuickLoop initialization is an automatic two-pass process that includes:

1. Sequential looplet initialization, where each device in a looplet registers with a switch.
2. Full QuickLoop initialization, which assigns a unique AL-PA to each device and starts QuickLoop operations.

Sequential Looplet Initialization

Each QuickLoop device obtains a unique AL_PA in a single AL_PA space. Only looplets from which Loop Initialization Procedure (LIPs) are received are initialized using the loop initialization procedure described in FC-AL. AL_PAs of devices in looplets from which no LIPs are received are preserved during the initialization. The sequential looplet initialization involves:

- Propagating LIPs to all looplets and forcing them into the OPEN-INIT state.
- Collecting an AL_PA bitmap super set that includes all AL_PAs in looplets from which no LIPs are received.
- Initializing the loop as described in FC-AL and using the AL_PA bitmap super set to initialize a looplet from which LIPs are received.
- Adding the AL_PAs of the newly initialized looplet to the AL_PA bitmap super set. If the newly initialized looplet has a hard-assigned AL_PA in conflict with a soft-assigned AL_PA of another looplet, the soft-assigned AL_PA is reinitialized.

Full Initialization

Full initialization sets up QuickLoop as a single logical PLDA. This process makes all assigned AL_PAs addressable by any device in a looplet regardless of whether the destination device and the source device are in the same physical looplet.

If the destination device is not in the same physical looplet as the source device, the hidden FL_Port in the source device looplet acts on behalf of the destination device. The hidden FL_Port in the destination device looplet acts on behalf of the source device while the fabric provides the transport service. Devices that are not physically located in a looplet but are addressable by a local device in the looplet are called phantom devices.

Operations performed during full initialization include:

- Initialization of all looplets
- Setting phantom devices in each looplet
- Setting the transport paths across all looplets
- Reinitializing all looplets to an operational state

QuickLoop Master

In a dual-switch QuickLoop, only one switch can drive the initialization process. The switch that drives a QuickLoop initialization is called the QuickLoop Master. Switches use the following criteria to elect the QuickLoop Master:

- If one of the switches receives LIPs from one (or more) of its looplets and the other switch does not, the switch that receives the LIPs becomes the QuickLoop Master.
- If both of the switches receive LIPs from their respective looplets, the switch that has the lower Domain ID becomes the QuickLoop Master.

NOTE: A dual-switch QuickLoop configuration requires that both switches have a Fabric Operating System license installed.

NOTE: The role of the QuickLoop Master is not fixed in one switch. It is determined dynamically each time the QuickLoop is initialized.

Address Translation

Address translation is achieved through hardware translative mode or phantom mode. A phantom device is a device that is addressable by a unique AL_PA (called phantom AL_PA) in a looplet, but not physically located in the local looplet. The phantom device is in the same fabric as the local looplet.

- Standard Translative Mode allows public devices to communicate with private initiator devices across the fabric.
- QuickLoop Mode allows private devices to communicate with other private devices across the fabric.
- Devices connected to a U_Port in QuickLoop mode are treated strictly as private devices, even if they are FLA capable devices. The QuickLoop-enabled U_Port drops the class 3 FLOGI if an NL_Port sends one.
- QuickLoop uses the Translative Mode of the switch to achieve the physical connection transparency.

Operation Modes

The operation modes are managed with Telnet commands. The system configuration has three control levels:

- **Fabric mode**—No U_Port participates in any logical PLDAs and all U_Ports operate as FC-FLA-compliant devices (default mode). This is level 1: fabric level.
- **QuickLoop mode**—All U_Ports participate in a logical PLDA (or dual-switch), unless a U_Port is overridden by a level 3 configuration. This is level 2: switch level.
- **Mixed mode**—Per port configuration that overrides level 2 configurations and can be set during installation. U_Ports can be configured as part of a logical PLDA (QuickLoop mode) or as a standard U_Port within the switch. This is level 3: port level.

NOTE: Operation modes cannot be configured through SNMP.

Configurations

QuickLoop supports two basic configurations:

- **Single-switch**—All looplets of a QuickLoop reside in one switch.
- **Dual-switch**—Looplets of a QuickLoop span two cascaded switches.

Both configurations allow up to 126 NL_Port devices in one QuickLoop. In addition to the two basic configurations, QuickLoop can be scaled to coexist within a fabric. In this case, you can reconfigure some of the original QuickLoop looplets to become fabric ports (F_Ports or FL_Ports), and additional fabric switches can be added as QuickLoop switches.

In a mixed QuickLoop and fabric configuration, fabric devices (public) can access QuickLoop devices (private) but not vice versa. There can be multiple QuickLoops within a fabric and each can be either single-switch or dual-switch. However, devices in different QuickLoops cannot communicate with each other.

Sample Configurations

The following figures show possible QuickLoop configurations. In each example, the dotted lines represent the logical QuickLoop or the ports that form the QuickLoop.

Configuration 1

Figure 5-1 shows a high-performance multi-initiator and multitarget connectivity to a single logical PLDA where the entire switch operates in QuickLoop mode. The switch serves as a concentrator, similar to a hub, offering throughput performance on each looplet of 100 MB/s.

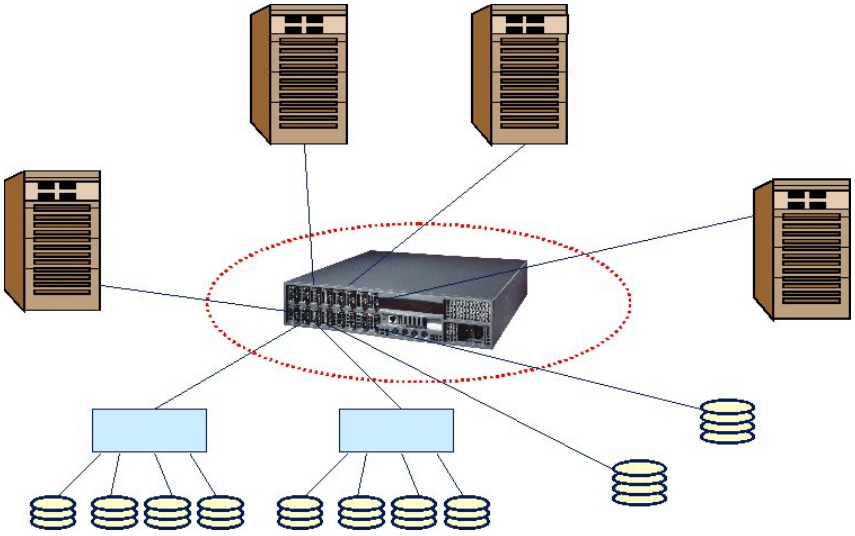


Figure 5-1. QuickLoop configuration example 1

Configuration 2

Figure 5-2 shows two cascaded switches in a single logical PLDA. The switches operate in QuickLoop mode and interconnect devices separated by a distance up to 10 km.

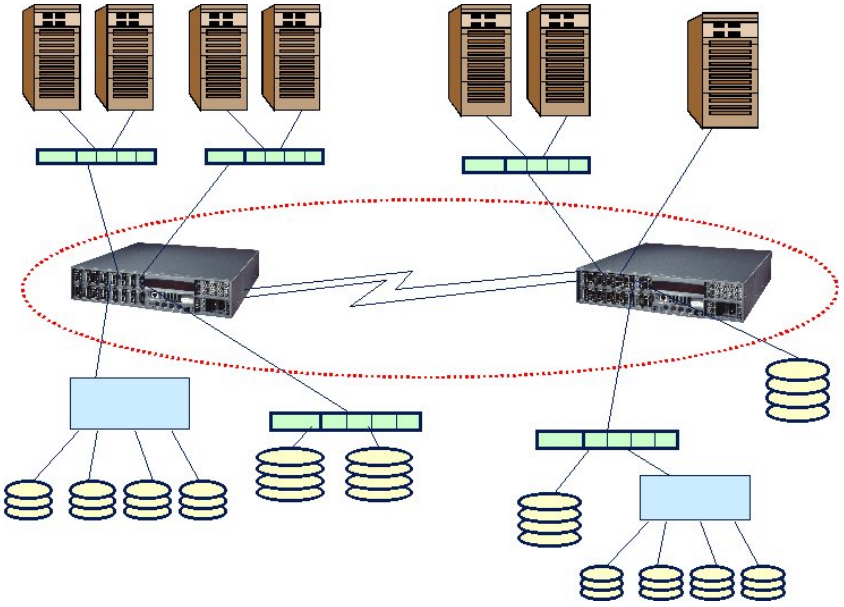


Figure 5-2. QuickLoop configuration example 2

Fault Isolation

A QuickLoop configuration can consist of multiple looplets across one or two switches. Fault isolation minimizes the impact of faulty looplets or switches on the normal QuickLoop functions.

Fault isolation occurs at two levels:

- Switch Level
- Port Level

Switch Level

In a dual-switch QuickLoop, the following conditions will trigger a fault:

- No switch configured with the partner switch's WWN is found in the fabric.
- No response was received from the partner switch during initial communication.
- An inconsistent response was received from the partner switch
- The response from the partner was not received in time during the QuickLoop initialization.

When a looplet is determined to be faulty, the entire port is bypassed and is prevented from initializing.

Port Level

The following conditions are considered faults as related to looplets:

- A U_Port fails to become the Loop Initialization Master (of the local looplet) within a time limit after LIPs are received from or sent to the port.
- A loop initialization sequence is not received by a U_Port within a time limit after the same sequence is sent.
- The frequency of LIPs received from a U_Port exceeds a threshold.
- Physical level errors exist, such as loss of sync, laser fault, and so on.

When a looplet is determined to be faulty, the port is bypassed and is prevented from initializing.

Recovery

If a switch or a U_Port diagnosed as faulty later recovers, it must be able to participate in the QuickLoop. If two previously disconnected partner switches, each containing QuickLoop with a set of private devices, are cascaded, the two switches reform a single QuickLoop containing both sets of private devices.

QuickLoop Zoning

The Fabric Operating System supports Zoning within QuickLoops (QuickLoop Zoning) for switches configured with both QuickLoop and Zoning. QuickLoop Zoning lets you:

- Segment a QuickLoop into separate, independent loops. You can use QuickLoop Zoning to build multiple loops within a single switch or QuickLoop switch-pair.
- Limit the scope of LIP propagation to only those looplets in the same zone. A looplet refers to the devices attached to a single switch port. QuickLoop Zoning ensures that all LIPs do not affect operation on unrelated looplets.
- Zone QuickLoops by port or by AL_PA. QuickLoop zone members cannot be specified by device WWNs.

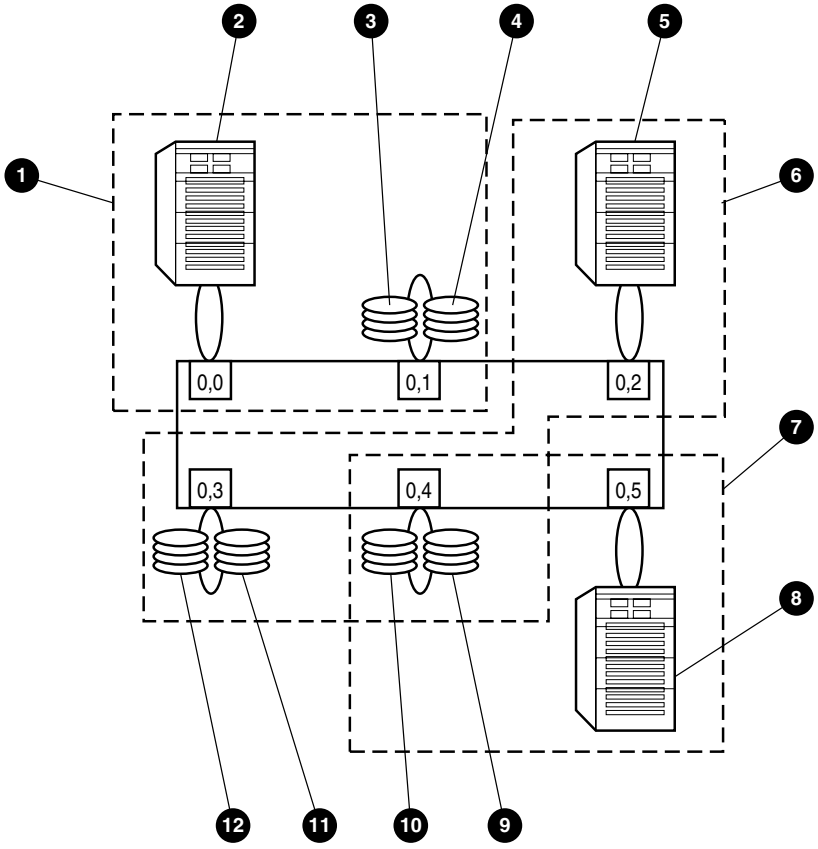
Limitations

- AL_PA Zoning can only be used on a single QuickLoop on the fabric. Only 1 QuickLoop can be configured on a fabric.
- Though QuickLoop allows you to create separate, independent loops within a QuickLoop, there is a single AL_PA address space within a single QuickLoop. Devices with hard AL_PAs must have unique AL_PAs within a QuickLoop.
- All QuickLoop zone members must be attached to a QuickLoop port, for example, QuickLoop 2.1.7 does not support Public devices on Fabric ports within a QuickLoop zone. Zones that do not contain AL_PAs whose members are defined by ports and WWNs can include public devices and private targets on a QuickLoop.
- If you enable QuickLoop Zoning by defining an AL_PA list then all switches must be v2.1.7 or the fabric will segment.
- If WWN are used for zoning, the QuickLoop devices do not have to be explicitly zoned. You can use WWN to zone the public devices without creating a zone for the QuickLoop.
- If hard zoning (domain, port) is used to zone the public devices, the QuickLoop devices must also be zoned through hard zoning.

Table 5-2
Hard Zoning Rules

Zoning	AL_PA	Port	WWN
Public zoning	No	Yes	Yes
QuickLoop zoning	Yes	Yes	No

A QuickLoop Zone limits the scope of LIP propagation and QuickLoop initialization. This scope is determined dynamically upon each LIP incidence and the source of the LIP. A LIP is sent to the smallest possible number of looplets.


1
2
3
4
5
6
7
8
0,0
0,1
0,2
0,3
0,4
0,5
12
11
10
9

In Figure 5-3, three QuickLoop zones have been defined. The notation is <switch #, port #>.

- qlZone1 includes ports 0,0 and 0,1
- qlZone2 includes ports 0,2, 0,3, and 0,4
- qlZone3 includes ports 0,4 and 0,5

In this example, qlZone2 and qlZone3 have overlapping zone members (0,4). qlZone1 is an exclusive zone such that its ports are exclusively in a single zone.

- Host A will receive the map of devices associated with ports 0,0 and 0,1, for instance, AL_PA [b8, c0, c1]. The map is used to indicate what devices are part of the loop.
- Host C will receive the map of devices associated with ports 0,2, 0,3, and 0,4, for instance, AL_PA [ba, e0, e1, e2, e3].
- Host B will receive the map of devices associated with ports 0,4 and 0,5, for instance, AL_PA [b9, e2, e3].
- LIP initiated within qlZone1 will only be propagated to ports 0,0 and 0,1.
- LIPs initiated within qlZone 2 or qlZone3 will be propagated to ports 0,2, 0,3, 0,4, and 0,5—the union of all ports in common zones.

Whenever a zone is changed or reconfigured, a LIP is generated to all affected looplets to indicate the configuration change. Configuring a QuickLoop Zone uses the same interfaces (Telnet or Web Management Tools) as are used for standard zones. However:

- Only switch ports can be used. QuickLoop zones cannot be configured with WWNs.
- The selected ports must all be in the corresponding switches (single switch or QuickLoop switch-pair) comprising the QuickLoop.
- Only QuickLoop ports can be configured. If fabric ports are included, it is not a QuickLoop Zone.

QuickLoop Zones using AL_PAs

AL_PA Zoning allows zone members to be designated by their AL_PA and is typically used for devices with hard AL_PAs. AL_PA Zoning has the convenience that zoning is still effective if the connection to the switch is changed from any one port to any other port. However, it can be more complex to manage.

Specifying an AL_PA will indirectly cause LIPs to be received on all devices contained within its corresponding looplet. For example, if you configure qlZone4 to include AL_PAs [b9, e3] in Figure 5-3, then the device with AL_PA [e2] will also receive the LIP because it is on the same looplet as device [e3]. However, the map returned to Host C will be [b9, e3] and the host will not be able to send frames to device e2.

There are four methods to create a QuickLoop Zone with AL_PA components using Telnet commands:

- Create a zone to include multiple AL_PAs as a list in square brackets:

  zoneCreate "qlzone3", "[b9, e3]"

- Zones can include both ports and AL_PA components. Separate components by semi-colon:

  zoneCreate "qlzone3", "0.1;[80]"

- An AL_PA list can be specified, in which case, all AL_PAs in the list will be included.

  zoneCreate "qlzone3", "0,1;[80,81,82,83,84,85,86,87,88]"

- AL_PAs can also be included in alias definitions.

  aliCreate "host_group1", "[80,81,82,83,84,85,86,87,88]"

Table 5-3
Valid AL_PAs

0x00	0x01	0x02	0x04	0x08	0x0f				
0x10	0x17	0x18	0x1b	0x1d	0x1e	0x1f			
0x23	0x25	0x26	0x27	0x29	0x2a	0x2b	0x2c	0x2d	0x2e
0x31	0x32	0x33	0x34	0x35	0x36	0x39	0x3a	0x3c	
0x43	0x45	0x46	0x47	0x49	0x4a	0x4b	0x4c	0x4d	0x4e
0x51	0x52	0x53	0x54	0x55	0x56	0x59	0x5a	0x5c	
0x63	0x65	0x66	0x67	0x69	0x6a	0x6b	0x6c	0x6d	0x6e
0x71	0x72	0x73	0x74	0x75	0x76	0x79	0x7a	0x7c	
0x80	0x81	0x82	0x84	0x88	0x8f				
0x90	0x97	0x98	0x9b	0x9d	0x9e	0x9f			
0xa3	0xa5	0xa6	0xa7	0xa9	0xaa	0xab	0xac	0xad	0xae
0xb1	0xb2	0xb3	0xb4	0xb5	0xb6	0xb9	0xba	0xbc	
0xc3	0xc5	0xc6	0xc7	0xc9	0xca	0xcb	0xcc	0xcd	0xce
0xd1	0xd2	0xd3	0xd4	0xd5	0xd6	0xd9	0xda	0xdc	
0xe0	0xe1	0xe2	0xe4	0xe8	0xef				

Chapter 6

Understanding and Using Zoning

This chapter covers the following topics:

- Overview of the SAN Switch Zoning
- Specifications
- Components
- Management
- Adding multiple items
- Enforcing a zone with software
- Enforcing a zone with hardware
- Multiswitch fabrics
- Adding a new switch
- Adding a new fabric
- Merging two fabrics
- Splitting a fabric

Overview

Zoning is a fabric management service used to create logical device subsets within a SAN. Zoning enables resource partitioning for management and access control.

One or more Fibre Channel switches create the Fibre Channel fabric, an intelligent infrastructure that serves as a backbone for deploying and managing information technology (IT) resources as a network. With Zoning, you can arrange fabric connected devices into logical groups over the physical fabric configuration.

Zoning provides automatic and transparent management for the SAN, and allows you the flexibility to allocate pools of storage in the SAN to meet different closed user group objectives. By creating zones of storage and computers, you can set up barriers between different operating environments to deploy logical fabric subsets or to create, test, and maintain separate areas within the fabric. Zoning lets you:

- Increase environmental security
- Optimize information technology (IT) resources
- Customize environments
- Easily manage a SAN

The following figure shows a typical use of Zoning.

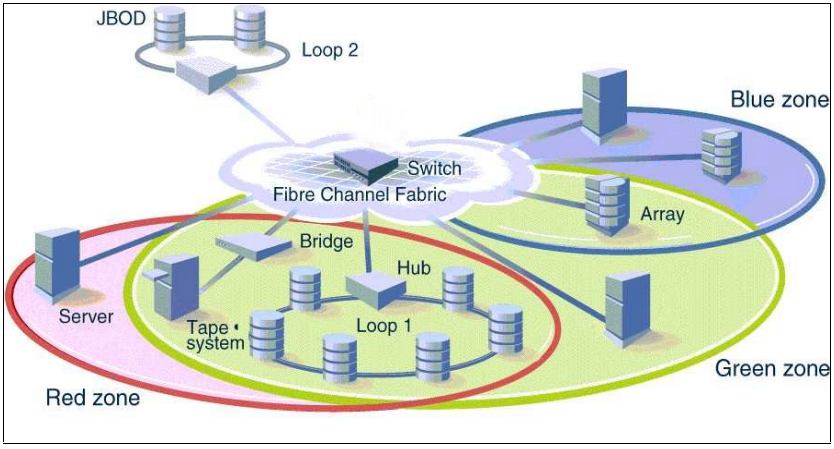


Figure 6-1. A fabric with three zones

Increased Security

The Fibre Channel fabric provides fast, reliable, and seamless information access within the SAN. Zoning lets you segment the fabric into zones that are comprised of selected storage devices, servers, and workstations. Since zone members can only see other members in the same zone, you can control access to computers and storage located in specific zones.

Optimized Resources

Zoning helps you optimize IT resources in response to user demand and changing user profiles. You can logically consolidate equipment for convenience. Zoning fabric characteristics are the same as other fabric services:

- Administration from any fabric switch
- Automatic, transparent distribution of zone definitions throughout the fabric—A single failure cannot interrupt Zoning Enforcement to other SAN connections.
- Automatic service scaling with fabric size—There is no requirement to upgrade systems as switches are added and connectivity increases.
- Automatic, transparent deployment—There is no requirement for human intervention unless the Zoning Specification must change.

Customized Environments

Zoning lets you customize your SAN environment. With Zoning, you can:

- Integrate support for heterogeneous environments by isolating systems that have different operating environments or uses.
- Create functional fabric areas by separating test or maintenance areas from production areas.
- Designate closed user groups by allocating certain computers and storage, such as RAID disks, arrays, and tapes, to a zone for exclusive use on computers that are zone members.
- Simplify resource utilization by consolidating equipment logically for convenience.
- Facilitate time-sensitive functions by creating a temporary zone to back up a set of devices that are members of other zones.
- Secure fabric areas by controlling port-level access.

Specifications

Web-based management and Telnet commands are used to create, delete, and display zones, to add or remove zone members, and to configure zone sets. Zone specification functions are:

- Administration
- Zone enforcement
- Zone management
- Zone backup

Table 6-1 summarizes the zone specification functions.

Table 6-1
Zone Specification Functions

Function	Description
Administration	Lets you create, delete, and display zones, zone members, and aliases.
Zone Enforcement	Automatically and transparently restricts access to only the devices in defined zones (provided by the fabric Simple Name Server) and hardware at the switch port level.
Zone Management	Lets you manipulate zones through Telnet commands.
Zone Backup	Automatically retains Zoning configuration data in the switch's flash memory.

Components

Zoning is comprised of three components. Table 6-2 summarizes the components and their hierarchical relationship.

Table 6-2
Zoning Components

Component	Description
Zone configuration	A set of zones. When Zoning is enabled, one zone configuration is in effect.
Zone	A set of devices that access one another. All computers, storage, and other devices connected to a fabric can be configured into one or more zones.
Zone member	A device located within a zone.

Zone Configuration

A zone configuration is a set of one or more zones. When Zoning is enabled, one zone configuration is in effect. When a zone configuration is in effect, all zones that are members of that configuration are valid. You select the type of configuration you want to use.

Defined Configuration

The defined configuration is the complete set of all zone components that are defined in the fabric. There can be multiple zone configurations defined, although only one configuration can be in effect at a time. For example, you can use one configuration during normal operation and a second configuration can be enabled for nightly data backup. There can be inconsistencies in the definitions, such as zones or aliases that are referenced but not defined, or duplicate members. The defined configuration is the current state of the administrator's input.

Effective Configuration

The effective configuration is a single zone configuration that is currently enabled. The effective configuration is built when you enable a specified zone configuration. The switch automatically compiles the effective configuration when you execute the cfgEnable command. The switch checks for undefined zone names or zone alias names or other inconsistencies by expanding zone aliases, removing duplicate entries, and then building the effective configuration.

Saved Configuration

The saved configuration is a copy of the defined configuration and the name of the effective configuration that is saved in flash memory by the cfgSave command. There can be differences between the saved configuration and the defined configuration if you modify the configuration and do not save the changes. The switch automatically reloads the saved configuration on power up. If a configuration was enabled when it was saved, the same configuration is automatically re-enabled when you power up the switch. If no configuration is enabled when you execute the cfgSave command, no configuration is loaded when you power up.

Zone

Each zone has a case-sensitive name. Zone names begin with a letter that can be followed by any number of letters, digits, and underscore characters (_). Spaces are not allowed in zone names.

Zones have the following characteristics:

- Each zone has a member list consisting of one or more zone members. Empty zones are not allowed.
- The maximum number of zones and zone members is constrained by memory usage. Since these limits are far larger than the number of devices connected to a fabric, you can have an almost unlimited amount of zones and zone members.
- Saved zone definitions are persistent. The definition remains in effect across reboots and power cycles unless it is deleted or changed.
- A device can be a member of multiple zones.

Zone Aliases

Zone aliases simplify repetitive port number entries or World Wide Names (WWNs). A zone alias is a C-style name for one or more port numbers or WWNs. For example, the name "host" can be used as an alias for a computer with the WWN of 10:00:00:60:69:00:00:8a.

Zone Member

Zone members can be specified using one of the following notations:

- Node World Wide Name
- Port World Wide Name
- Physical fabric port number

A World Wide Name (WWN) notation (for node and/or port) is specified as an eight-hex number separated by colons, for example 10:00:00:60:69:00:00:8a. The number is compared with the node and port WWNs presented by a device in a login frame (FLOGI or PLOGI). When a zone member is specified by node WWN, all ports on that device are in the zone. When a zone member is specified by port name, only that port is in the zone.

A physical fabric port number notation is specified as a pair of decimal numbers s,p where s is the switch number (domain ID) and p is the switch port number. For example, 2,12 specifies port 12 on switch number 2. When a physical fabric port number specifies a zone member, all devices connected to that port are in the zone. If the port is an arbitrated loop, all loop devices on that port are in the zone.

The type of notation used to define zone members can be a combination of WWN and physical fabric port numbers. Consider a zone defined with the following members:

```
2,12; 2,14; 10:00:00:60:69:00:00:8a
```

The zone contains the devices connected to switch 2 at ports 12 and 14, as well as the device with the node name or port name of 10:00:00:60:69:00:00:8a.

Management

Zoning is managed using Web Management Tools or Telnet commands through either out-of-band or in-band communication by logging in to a switch. Any switch in the fabric can be used to manage zones. A change made to the Zoning information on one switch is replicated through all fabric switches. Zoning provides:

- Greater flexibility to manage a SAN with multiple operational objectives
- Easy allocation of computers and storage resources
- Finer configuration granularity to logically configure resources and seclude environments
- Versatility to meet dynamically changing application demands

Web Management Tools or Telnet commands can be used to create, delete, and display zones and zone members.

The Telnet commands are based on the three component types:

- Zone alias
- Zone configuration
- Zone

Each component type recognizes five commands:

- Create
- Delete
- Add
- Remove
- Show

Zone Management Example

This example shows a single zone configuration, USA_cfg, that has the following three zones defined:

- The Red and Green zones share six disk drives on a loop.
- The Blue and Green zones share one storage array.
- The Blue zone has a dedicated storage array.

NOTE: The JBOD with Loop 2 is not in a zone and cannot be accessed from outside of Loop 2 when the configuration is in effect.

The disks are specified by WWN and the hosts are specified by physical port. The graphical representation of the zone configuration includes an additional disk drive loop that none of the zones can access.

```
admin> cfgCreate "USA_cfg", "Red_zone; Blue_zone; Green_zone"
admin> zoneCreate "Red_zone", "0,0; loop1"
admin> zoneCreate "Blue_zone", "0,1; array1; 0,2; array2"
admin> zoneCreate "Green_zone", "0,0; loop1; 0,2; array2"
admin> aliCreate "array1", "21:00:00:20:37:0c:76:85;
21:00:00:20:37:0c:71:df"
admin> aliAdd "array1", "21:00:00:20:37:0c:72:51;
21:00:00:20:37:0c:71:0a"
admin> aliCreate "array2", "21:00:00:20:37:0c:66:23;
21:00:00:20:37:0c:73:7f"
admin> aliAdd "array2", "21:00:00:20:37:0c:9c:6b;
21:00:00:20:37:0c:66:3a"
admin> aliCreate "loop1", "21:00:00:20:37:0c:67:e3;
21:00:00:20:37:0c:76:1f"
admin> aliAdd "loop1", "21:00:00:20:37:0c:6a:40;
21:00:00:20:37:0c:59:7e"
admin> cfgEnable "USA_cfg"
zone config "USA_cfg" is in effect
```

Figure 6-2. Zone management example

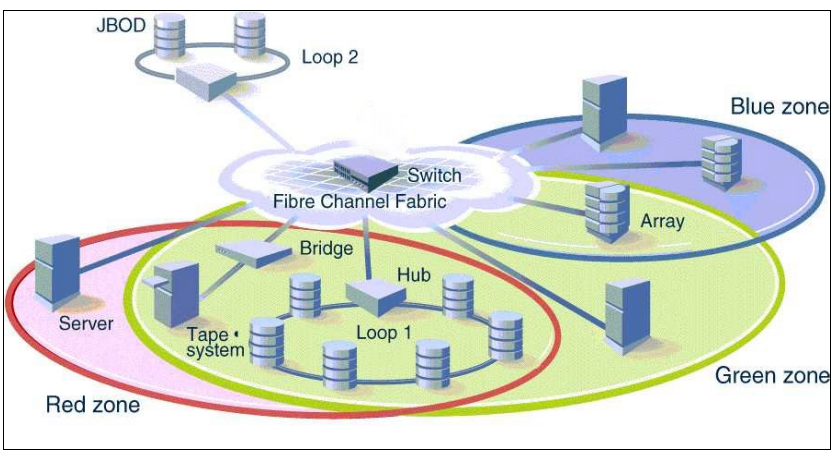


Figure 6-3. Zone management example

Adding Multiple Items

Multiple items can be added to a zone with the following command syntax:

```
zoning-command “name of zone”, “member; member; member”
```

The “name of zone” parameter can be a zone name, an alias name, or a configuration name depending on the type of command you are using. Consider the following example:

```
zoneAdd “Red_zone”, “1,10;1,12”
```

This syntax adds domain 1, port 10 and domain 1, port 12 to the Red zone. The following commands allow a multiple item parameter list.

- Alias commands: aliCreate, aliAdd, and aliRemove
- Zone configuration commands: cfgCreate, cfgAdd, and cfgRemove
- Zone commands: zoneCreate, zoneAdd, and zoneRemove

Enforcing a Zone with Software

A software implementation based on the Simple Name Server (SNS) enforces a zone when you use WWNs for Zoning devices. Zoning does not degrade SNS functionality because there is no change to the SNS access protocol. If no zone configuration is in effect, responses to SNS queries are based on all fabric connected devices. If a zone configuration is in effect, responses to SNS queries contain information about only those devices that are in the requestor’s zone.

Enforcing a Zone with Hardware

Zones are enforced at the physical port level across all fabric switches by hardware blocking of Fibre Channel frames. Hardware zoning enables computers and storage on different switch ports to communicate. You specify a zoned switch by using the physical fabric port number. Hardware zone definitions are in the form of D,P where D is the domain and P is the physical port number on a switch. Hardware zoning prevents computers and storage from communicating with devices that do not share a common zone.

Multiswitch Fabrics

Zoning uses two databases:

- The zone configuration database
- The N_Port login database

Zone Configuration Data

Zone configuration data is contained in a replicated database. All fabric switches have a complete copy of the zone configuration database. When you make a configuration change, a unique interswitch protocol forwards the change to all fabric switches. Zone configuration data is displayed as the defined configuration by the cfgShow command, and is stored in flash memory by the cfgSave command.

N_Port Login Data

N_Port login data is stored locally on each switch where it is used to translate WWNs into physical port numbers. The procedure runs entirely on the local switch when a match can be made based only on the physical port number. If the physical port number is not sufficient, the local switch queries the remote switch for login data.

Adding a New Switch

A new switch is a switch that has not previously been connected to a fabric and has no zone configuration data. When you connect a new switch to a fabric, all zone configuration data is immediately copied from the fabric to the new switch. If a zone configuration is enabled in the fabric, then the same configuration is enabled in the new switch.

NOTE: A switch that has previously been configured for Zoning can be returned to a new switch state by using the cfgClear command before connecting it to the fabric.

Adding a New Fabric

A new fabric is a fabric where there is no zone configuration information. When you add a new fabric to an existing zoned fabric, all switches in the new fabric inherit the zone configuration data from the existing zoned fabric. If a zone configuration is enabled, then the same configuration is enabled in the new switches.

Merging Two Fabrics

If both fabrics have identical zone configuration data and the same configuration is enabled, the fabrics join to make one larger fabric with the same zone configuration in effect.

If the fabrics have different zone configuration data, the two sets of information are merged when possible. Merging is not possible if:

- Zoning is enabled in both fabrics but the zone configurations that are enabled are different (cfg mismatch).
- The name of a zone object in one fabric is used for a different type of zone object in the other fabric (type mismatch).
- The definition of a zone object in one fabric is different from its definition in the other fabric (content mismatch).

The interswitch link (ISL) is segmented if a merge is not possible. When a segmented condition is detected by the switches between the ISL, each switch displays an error message.

Configuration Mismatch

A mismatch can result if a zone definition is changed while a switch that was part of a zone fabric is powered down. To allow a switch with a zone mismatch to join a fabric, clear the zone definitions in the switch that has the wrong zone definition.

Splitting a Fabric

If an ISL goes down, causing a fabric to split into two separate fabrics, then each new fabric retains the same zone configuration.

If the ISL is replaced and no changes have been made to the zone configuration in either new fabric, then the two fabrics will merge back into one single fabric. If changes have been made to either zone configuration, the rules in the “Merging Two Fabrics” section apply.

Chapter 7

Upgrading Firmware

This chapter covers the following topics:

- Rolling upgrades
- Upgrading firmware:
  - Using Web Management Tools
  - Using a Telnet command
  - Downloading from the Compaq website
- Save and restore configuration

A Fibre Channel SAN Switch comes with preloaded firmware. In most cases there is no need to update the firmware on a new switch. The firmware version can be determined by using:

- The version Telnet command (see Appendix A, “Telnet Commands”)
- The front panel on a Fibre Channel SAN Switch 16 (see the manual that came with your switch)
- The Switch Management Application page in Web Management Tools (see Chapter 3, “Managing the Switch Using Web Management Tools”)

Rolling Upgrades

Because of a compatibility issue that affects the way switches are displayed in the TopZoneNS page, the Fibre Channel SAN Switch 8-EL will display as a Fibre Channel SAN Switch 8 on the TopZoneNS page. This will occur only in the TopZoneNS page; the correct switch graphics will be displayed elsewhere.

The compatibility issue occurs only when interconnecting switches with firmware v2.03a and Fibre Channel SAN Switch 8-EL switches with firmware v2.1.7 or later. In environments with switches at different firmware levels, the TopZoneNS page will not display any switches if the Web Management Tools is launched from a switch running firmware v2.03a.

In environments where all switches have firmware v2.1.7 or later, you may choose to change the way the Fibre Channel SAN Switch 8-EL icon is displayed in Fabric view page to the correct graphics. This can be accomplished by issuing the fakeModel Telnet command for Fibre Channel SAN Switch8-EL switches.

The default parameter for the Fibre Channel SAN Switch 8-EL is "3" which displays the Fibre Channel SAN Switch 8-EL as a Fibre Channel SAN Switch 8 in mixed firmware environments.

Set the fakeModel parameter to "0" which resets the Fibre Channel SAN Switch 8-EL to display the correct graphics in the TopZoneNS screen.

NOTE: This command should only be used to change the parameter to "0" when all switches are running firmware version v2.1.7 or later.

Upgrading Firmware Using Web Management Tools

Use the Firmware Upgrade page in Web Management Tools to download firmware upgrades.

To download the firmware:

1. Copy the files *Rshd.exe* and *Cat.exe* to the root directory on the host system. These files are found in:
   D:\DSGGB\Firmware\NTIntel\Rshd.exe
   D:\DSGGB\Firmware\NTIntel\Cat.exe
   D:\DSGGB\Firmware\NTIntel\V2.1.7

   where D:\ is the drive letter for the CD and V2.1.7 is the latest version of firmware.
2. Double-click *Rshd.exe*. RSHD is a server program that allows the switch to request the firmware from the host over an Ethernet connection. Leave RSHD running in a separate window.
3. Click the switch whose firmware you want to upgrade. The Switch Management Application page displays.
4. Click on the admin button from the Switch Management Application page.
5. Click on the Firmware Upgrade tab. The following screen is displayed:

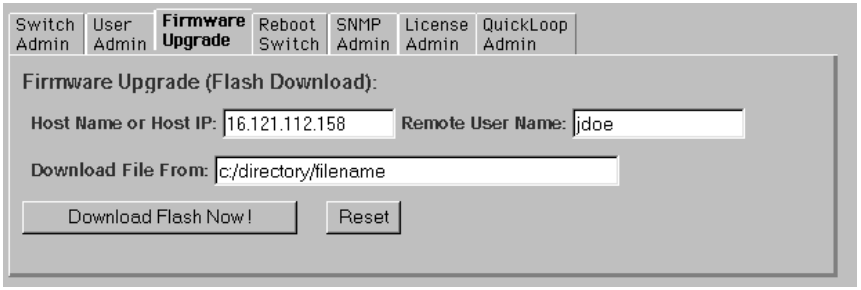


Figure 7-1. Firmware Upgrade page example

6. Enter the host name or host IP address in the Host Name or Host IP field.

   NOTE: For Windows 9x/Windows 2000/Windows NT only, enter the IP address.

7. Enter a user name in the Remote User Name field.

   NOTE: For Windows 9x, Windows 2000, and Windows NT only, enter the default name user.

8. In the Download File From field, enter the path name from which the firmware resides.

   IMPORTANT: You must use the UNIX style of forward slash (/) for the path name.

   NOTE: When the firmware file is located in the same directory as the *Cat.exe* and *Rshd.exe* files, the directory path can be omitted.

9. Click the Download Flash Now! button.

   IMPORTANT: Prior to downloading the firmware, the *Rshd.ex*e program must be running from the same directory that contains the *Cat.exe* program or the FTP server must be running.

The firmware is downloaded. Use this procedure for each switch to be upgraded.

Upgrading Firmware Using a Telnet Command

Use the firmwareDownload command in a Telnet session to download new firmware. The command downloads firmware into flash memory. This command can be executed on an operational switch. A reboot is required to initiate the new firmware after the download has completed.

The firmware can be downloaded from a Unix host, Windows 95 host, or Windows NT host. For a Unix host, no special software is needed. For Windows 95 or Windows NT, a daemon to support a Remote Shell is required. Firmware is downloaded through an RCP command running on top of TCP between the switch and the host.

To upgrade the firmware of a Fibre Channel SAN Switch, use the latest version of the Fibre Channel SAN Switch CD. Use one of the following three procedures (Windows NT Intel, Windows NT Alpha, or Tru64 UNIX).

Host with Windows NT Intel

To load the firmware from a Compaq PC running Windows NT Intel:

1. Copy the files *Rshd.exe* and *Cat.exe* to the root directory on the host system. These files are found in:
   D:\DSGGB\Firmware\NTIntel\Rshd.exe
   D:\DSGGB\Firmware\NTIntel\Cat.exe
   D:\DSGGB\Firmware\NTIntel\V2.1.7

   where D:\ is the drive letter for the CD and V2.1.7 is the latest version of firmware.

2. Double-click *Rshd.exe*. RSHD is a server program that allows the switch to request the firmware from the host over an Ethernet connection. Leave RSHD running in a separate window.

3. Click Start > Run and enter TELNET.

4. Click Connect > Remote System.

5. In the Host Name field, type the IP address of your Fibre Channel SAN Switch and click the Connect button.

6. Log in as:

   admin
   password: password

7. At the prompt, type:

   firmwareDownload "192.168.60.200", "administrator" , "v2.1.7"

   where "192.168.60.200" is the IP address of your host computer, "administrator" is the account you are using to run *Rshd.exe*, and "v2.1.7" is the firmware image to be downloaded to the switch.

   NOTE: *Rshd.exe* must be run from the directory that contains the *Cat.exe* file.

   The output displays as follows:

   1330320+203572+427356
   writing flash 0 .....
   writing flash 1 .....
   download complete
   switch:admin>

8. Click the RSHD window and click File > Exit.

9. Click the Telnet window and enter reboot. The switch reboots and copies the firmware into RAM.

Host with Windows NT Alpha

To load the firmware from a host running Windows NT Alpha:

1. Copy the files *Rshd.exe* and *Cat.exe* to the root directory on the host system. These files are found in:
   D:\DSGGB\Firmware\NTAlpha\Rshd.exe
   D:\DSGGB\Firmware\NTAlpha\Cat.exe
   D:\DSGGB\Firmware\NTAlpha\V2.1.7

   where D:\ is the drive letter for the CD and V2.1.7 is the latest version of firmware.
2. Double-click *Rshd.exe*. RSHD is a server program that allows the switch to request the firmware from the host over an Ethernet connection. Leave RSHD running in a separate window.
3. Click Start > Run and enter TELNET.
4. Click Connect > Remote System.
5. In the Host Name field, type the IP address of your Fibre Channel SAN Switch and click the Connect button.
6. Log in as:

   admin
   password: password
7. At the prompt, type:

   firmwareDownload "192.168.60.200", "administrator" , "v2.1.7"

   where "192.168.60.200" is the IP address of your host computer, "administrator" is the account you are using to run *Rshd.exe*, and "v2.1.7" is the firmware image to be downloaded to the switch.

   NOTE: *Rshd.exe* must be run from the directory that contains the *Cat.exe* file.

   The output displays as follows:

   1330320+203572+427356
   writing flash 0 .....
   writing flash 1 .....
   download complete
   switch:admin>
8. Click the RSHD window and click File > Exit.
9. Click the Telnet window and enter reboot. The switch reboots and copies the firmware into RAM.

Host with Tru64 UNIX

To load the firmware from a host running Compaq Tru64 UNIX:

1. Mount the CD device by using the following command:

   mount –t cdfs –r /dev/rz5c /mnt

2. Change to the CD directory by entering:

   cd mnt

3. To copy the firmware to the host system, enter the following command:

   cp DSGGB/Firmware/V2.1.7/mary/tmp/V2.1.7

   where mary is the user name on the Tru64 host system and V2.1.7 is the firmware image to be downloaded to the switch.

   NOTE: The Fibre Channel SAN Switch uses the remote shell capabilities of UNIX to log in to the Tru64 UNIX host and copy the firmware image. The user (mary) and the switch's IP address must be in the *.rhosts* file on the Tru64 UNIX host to allow login without a password.

4. Telnet to the switch by entering:

   telnet <switch_hostname>
   user: admin
   pswd: <password>

   NOTE: You can substitute the IP address of the switch for <switch_hostname>.

5. To download the firmware from the host system to the switch flash memory, enter the following command line at the <switch>:admin> prompt:

   firmwareDownload "16.140.32.60", "mary", "/tmp/v2.1.7"

   where "16.140.32.60" is the IP address of the host system with the firmware image, "mary" is the user to RSH, and "/tmp/v2.1.7" is the firmware image to be loaded into the switch flash ROM.

   NOTE:

   - The quote marks are very important in the firmwareDownload command line.
   - RSH without a password must be enabled for the user that RSH is executing under. To enable RSH without a password, add the switch IP name to ~<user>/.rhosts). The format of .rhosts is: hostname [user].

6. Enter reboot at the Telnet prompt. The switch reboots and copies the firmware into RAM.

Downloading Firmware from the Compaq Website

To download the firmware from the Compaq website, go to www.compaq.com/products/storageworks.

The website contains the required loaders and instructions for downloading the firmware into a switch.

Save and Restore Switch Configuration Settings

Configuration settings can be lost upon switch failure. It is recommended that you save your switch configuration settings using the configUpload Telnet command. In order to restore your saved configuration settings, use the configDownload Telnet command.

configUpload

This command saves the switch configuration to a host file. The upload process uses either FTP (File Transfer Protocol) or the RSHD protocol (TCP service 514). Both of these services are widely available on Unix hosts, but less so on Microsoft Windows hosts.

On Windows NT, the FTP server may have to be installed from the distribution media and enabled, or on Windows NT or Windows 9x there are several good freeware and shareware FTP servers available.

The two utilities supplied for RSHD, *Rshd.exe* and *Cat.exe*, currently **do not** support uploads, only downloads. Therefore, in a Windows environment, FTP must be used and the FTP server must be running before an upload can occur.

The command may be invoked without any parameters, in which case the user is prompted for input, including choice or FTP or RSHD. If invoked with three parameters RSHD is used, otherwise presence of the fourth parameter (FTP password) selects FTP.

Figure 7-2 shows a generic example of the configUpload command.

```
switch:admin>configUpload
Server Name or IP Address [host]:
IP Address for Server:
User Name [user]:
File Name [config.txt]:
Protocol (RSHD or FTP) [rshd]:
```

Figure 7-2. configUpload command example 1

If the upload fails, it is due to one of the following reasons:

- The switch does not recognize the host name.
- The host IP address can't be contacted.
- The user doesn't have permission on the host.
- The user runs a script that prints something at login.
- The RSHD or FTP server is not running on the host.

The configuration file contains two types of lines, comments and name:value pairs. Comments are written with "[" as the first character of the line (when read back using configDownload, a line beginning with any punctuation character is treated as a comment).

Table 7-1
Syntax of a Name:Value Pair

Name	Value Pair
line	whitespace name whitespace ":" whitespace value
name	component {"." component}
whitespace	{" " | " "}
component	{"a"-"z" | "A"-"Z" | "0"-"9" | "_" | "-"}
value	{<any character not including "

Note: Elements enclosed in curly braces ({...}) indicate zero or more occurrences of the enclosed elements.

The configuration file is written as three sections. The first section contains the switch boot parameters (otherwise known as the switch's identity). It has variables such as the switch's name and IP address. This section corresponds to the first few lines of output of the configShow command.

The second section contains general switch configuration variables, such as diagnostic settings, fabric configuration settings, and SNMP settings. This section corresponds to the output of the configShow command (after the first few lines), although there are more lines uploaded than shown by the command.

The third section contains the zoning configuration. It corresponds to the output of the cfgShow command.

Parameters

- host—A host name or IP address in quotes, for example "citadel" or "192.168.1.48". The configuration file is uploaded to this host.
- user—A user name in quotes, for example "jdoe." This user name is used to gain access to the host.
- file—A file name in quotes, for example "config.txt." Absolute path names may be specified using forward slash "/". Relative path names create the file in the user's home directory on Unix hosts and in the directory where the FTP server is running on Windows hosts.
- passwd—If present, selects FTP.

```
switch:admin>configUpload
“citadel”,“jdoe”,“config.txt”,“passwd”
upload complete
```

Figure 7-3. configUpload command example 2

configDownload

The download process uses either FTP or the RSHD protocol (TCP service 514) to download a previously saved configuration file from a host system into the switch. Both of these services are widely available on Unix hosts, but less so on Windows hosts. See the Telnet configUpload command for a description of the configuration file format.

On Windows NT, the FTP server may have to be installed from the distribution media and enabled. There are several good freeware and shareware FTP servers available for Windows NT, Windows 9x, and Windows 2000.

To use RSHD on Windows NT, Windows 9x, or Windows 2000, two utilities are supplied, *Rshd.exe* and *Cat.exe*. The FTP server or RSHD must be running before a download can occur.

The command may be invoked without any parameters, in which case the user is prompted for input, including choice or FTP or RSHD. If invoked with three parameters RSHD is used, otherwise presence of the fourth parameter (FTP password) selects FTP. Figure 7-4 shows a generic example of the configDownload command.

```
switch:admin>configDownload
Server Name or IP Address [host]:
IP Address for Server:
IP Address for Server:
IP Address for Server:
User Name [user]:
File Name [config.txt]:
Protocol (RSHD or FTP) [rshd]:
```

Figure 7-4. configDownload command example 1

If the download fails, it is due to one of the following reasons:

- The switch does not recognize the host name.
- The host IP address can't be contacted.
- The user does not have permission on the host.
- The user runs a script that prints something at login.
- The file doesn't exist on the host.
- The file is not a switch configuration file.
- The RSHD or FTP server is not running on the host.
- The configuration data contains errors.

NOTE: The switch's identity cannot be changed by configDownload. Parameters such as the switch's name and IP address are ignored. They are the lines in the configuration file, which begin "boot".

NOTE: A licenseKey is only accepted if the boot.mac line matches the WorldWide Name of the switch performing the download, otherwise it is ignored..

The download process is additive, for example, the lines read from the file are added to the current switch configuration. It is therefore possible to change a single configuration variable by downloading a file with a single line. All other variables remain unchanged.

This is particularly important to understand when downloading a zoning configuration. Since the new zoning information is added to the current configuration there may not be any conflicts. If the current zoning configuration is to be replaced, then the key word "clear:" may be inserted into the configuration file immediately before the zoning lines.

Parameters

- host—A host name or IP address in quotes, for example "citadel" or "192.168.1.48". The configuration file is downloaded from this host.
- user—A user name in quotes, for example "jdoe." This user name is used to gain access to the host.
- file—A file name in quotes, for example "config.txt." Absolute path names may be specified using forward slash "/". Relative path names look for the file in the user's home directory on Unix hosts and in the directory where the FTP or RSHD server is running on Windows hosts.
- passwd—If present, selects FTP.

```
switch:admin>configDownload
“citadel”,“jdoe”,“config.txt”
Committing configuration…done.
download complete
```

Figure 7-5. configDownload command example 2

Appendix **A**

Telnet Commands

Introduction

This appendix contains information and examples on managing and monitoring Compaq StorageWorks Fibre Channel SAN Switches using Telnet with:

- QuickLoop-specific commands
- Fabric Operating System and QuickLoop commands:
  - General commands
  - Diagnostic commands
  - Routing commands
  - License commands
- Zoning-specific commands

You can configure, operate, and test the switch using the following commands and settings through the Telnet interface.

NOTE: Screen displays in this appendix are generic. Your display will vary depending on your configuration, licenses, and port type.

QuickLoop-Specific Telnet Commands

QuickLoop-specific Telnet commands let you manage the QuickLoop topology.

qlDisable

Figure A-1 shows the qlDisable command, which disables QuickLoop on a switch with a Fabric Operating System license. This command resets the switch to fabric mode and re-enables the ports as U_Ports.

```
admin> qlDisable
Setting switch to Fabric mode,
Committing configuration...done.
Re-enable FL_Ports
```

Figure A-1. qlDisable command example

qlEnable

Figure A-2 shows the qlEnable command, which enables QuickLoop on a switch with a Fabric Operating System license. This command sets the switch to QuickLoop mode.

```
admin> qlEnable
Setting switch to QuickLoop mode,
Committing configuration...done.
Initialize QuickLoop
```

Figure A-2. qlEnable command example

qlPortDisable

Figure A-3 shows the qlPortDisable command, which sets a port on a switch with a Fabric Operating System license to fabric mode.

```
admin> qlPortDisable 6
Setting port to Fabric mode,
Committing configuration...done.
De-activate looplet 6
```

Figure A-3. qlPortDisable command example

qlPortEnable

Figure A-4 shows the qlPortEnable command, which sets a port on a switch with the Fabric Operating System license to QuickLoop mode.

```
admin> qlPortEnable 6
Setting port to QuickLoop mode,
Committing configuration...done.
Activate looplet 6
```

Figure A-4. qlPortEnable command example

qlOnlineHold

Figure A-5 shows the qlOnlineHold command, which sets hold loop in the Monitoring state option for QuickLoop. It affects the starting loop state of pass1 QuickLoop initialization. The parameter can be set to "0" or "1". When set to "1", the looplet starts pass1 initialization from its existing state. When set to "0", the looplet starts from open_init state.

qlOnlineHold sets the option only. The command does not start loop initialization. The setting updates in the flash and remains in effect until the next change.

```
admin> qlonlinehold 0
Committing configuration.done

admin> qlonlinehold
Current setting is: FALSE

admin> qlonlinehold 1
Committing configuration.done

admin> qlonlinehold
Current setting is: TRUE
```

Figure A-5. qlOnlineHold command example

qlOpenInitHold

Figure A-6 shows the qlOpenInitHold command. The parameter can be set to "0" or "1". When set to "1', QuickLoop initialization will hold a looplet in the Open_init state during pass 1 of the QuickLoop initialization. If set to "0", QuickLoop initialization will keep a looplet in the Monitoring state during pass 1 of the initialization. The default setting is "0".

```
admin> qlopeninithold 0
Committing configuration…done

admin> qlopeninithold
Current setting is: FALSE

admin> qlopeninithold 1
Committing configuration…done

admin> qlopeninithold
Current setting is: TRUE
```

Figure A-6. qlOpenInitHold command example

qlPartner

Figure A-7 shows the qlPartner command, which prints and sets the QuickLoop partner. For a dual-switch QuickLoop, both switches must have the Fabric Operating System license installed. Issue the qlPartner command on both switches by including the remote switch's WWN. To set QuickLoop in single-switch mode, include a zero (0) with the command.

```
admin> qlPartner 0
Setting QuickLoop to single-switch mode,
Committing configuration...done.

admin> qlPartner
QuickLoop is in single-switch mode, partner is not specified.

admin> qlPartner "10:00:00:60:69:10:02:0d"
Setting QuickLoop to dual-switch mode,
Committing configuration...done.

admin> qlPartner
QuickLoop is in dual-switch mode, partner is
10:00:00:60:69:10:02:0d.
```

Figure A-7. qlPartner command example

qlShow

Figure A-8 shows the qlShow command, which displays the current QuickLoop configuration. In this example, QuickLoop is in the dual-switch mode. Table A-1 describes the command fields.

NOTE: Port 10 is missing as part of the QuickLoop configuration because port 10 is actually an E_Port cascaded to another switch.

```
admin> qlShow
Self:       10:00:00:60:69:10:02:09 domain 1
Peer:       10:00:00:60:69:10:02:0d domain 2
State:      Master
Scope:      dual
AL_PA bitmap:  18000000 00000000 00000000 000000ff
Remote AL_Pas
[021600]:     e2 e4 e8 ef
[021700]:     04
[021900]:     da dc e0 e1
Local AL_Pas
[011900]:     02
Local looplet states
Member: 0   1   2   3   4   5   6   7   8   9   11  12  13  14  15
Online:  -   -   -   -   -   -   -   -   -   9   -   --  --  --  --
Looplet 0:    offline
Looplet 1:    offline
Looplet 2:    offline
Looplet 3:    offline
Looplet 4:    offline
Looplet 5:    offline
Looplet 6:    offline
Looplet 7:    offline
Looplet 8:    offline
Looplet 9:    online
Looplet 11:   offline
Looplet 12:   offline
Looplet 13:   offline
Looplet 14:   offline
Looplet 15:   offline
```

Figure A-8. qlShow command example

Table A-1
qlShow Command Field Descriptions

Field	Description
Self	The local switch with its WWN and domain number
Peer	The remote switch with its WWN and domain number (if QuickLoop is in a dual-switch mode)
State	Indicates if the local switch is the master or nonmaster
Scope	Indicates if the QuickLoop mode is dual or single
AL_PA bitmap	All AL_PAs in the QuickLoop
Remote AL_PAs	The looplets and devices in QuickLoop mode on the remote switch
Local AL_PAs	The looplets and devices in QuickLoop mode on the local switch
Local looplet states	The looplets, member switch ports, online QuickLoop ports, and looplet port status

qlHelp

Figure A-9 shows the qlHelp command, which displays a list of QuickLoop commands.

```
admin> qlHelp
qlDisable          Disable QuickLoop mode
qlEnable           Enable QuickLoop mode
qlPortDisable      Set port in non QuickLoop mode
qlPortEnable       Set port in QuickLoop mode
qlPartner          Print/set QuickLoop partner
qlShow             Print QuickLoop info
```

Figure A-9. qlHelp command example

Fabric Operating System and QuickLoop Telnet Commands

General Commands

General commands let you control basic switch operations.

agtcfgSet

Figure A-10 shows the agtcfgSet command, which is used to set the SNMP agent configuration to a Fibre Channel switch. Table A-2 describes the fields.

NOTE: Any change to the SNMP configuration is not shown until you reboot the switch.

```
admin> agtcfgSet

Customizing MIB-II system variables ...

At each prompt, do one of the following:
   0  <Return> to accept current value,
   0  enter the appropriate new value,
   0  <Control-D> to skip the rest of configuration, or
   0  <Control-C> to cancel any change.

To correct any input mistake:
<Backspace> erases the previous character,
<Control-U> erases the whole line,
sysDescr: [Fibre Channel Switch]
sysLocation: [End User Premise]
sysContact: [Field Support]
authTrapsEnabled (true, t, false, f): [false]

SNMP community and trap recipient configuration:
Community: [Secret C0de]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community: [OrigEquipMfr]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community: [private]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community: [public]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community: [common]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community: [FibreChannel]
Trap Recipient's IP address in dot notation: [0.0.0.0]
```

Figure A-10. agtcfgSet command example

agtcfgShow

Figure A-11 shows the agtcfgShow command, which displays the SNMP agent configuration. The fields are described in Table A-2.

```
admin> agtcfgShow
Current SNMP Agent Configuration
Customizable MIB-II system variables:
    SysDescr     = Fibre Channel Switch
    SysLocation  = End User Premise
    SysContact   = Field Support
    AuthTraps    = 0 (OFF)

SNMPv1 community and trap recipient configuration:
   Community 1: Secret C0de (rw)
      No trap recipient configured yet
   Community 2: OrigEquipMfr (rw)
      No trap recipient configured yet
   Community 3: private (rw)
      No trap recipient configured yet
   Community 4: public (ro)
      No trap recipient configured yet
   Community 5: common (ro)
      No trap recipient configured yet
   Community 6: FibreChannel (ro)
      No trap recipient configured yet
```

Figure A-11. agtcfgShow command example

agtcfgDefault

Figure A-12 shows the agtcfgDefault command, which lets an admin user reset the configuration of the SNMP agent to factory defaults. Table A-2 describes the fields.

```
switch:admin> agtcfgDefault
Committing configuration...done.
agent configuration reset to factory default
sw5:admin> agtcfgShow
Current SNMP Agent Configuration
Customizable MIB-II system variables:
    SysDescr          =  Fibre Channel Switch
    SysLocation       =  End User Premise
    SysContact        =  Field Support
    SwEventTrapLevel  =  0
    AuthTraps         =  0 (OFF)

SNMPv1 community and trap recipient configuration:
   Community 1: Secret C0de (rw)
      No trap recipient configured yet
   Community 2: OrigEquipMfr (rw)
      No trap recipient configured yet
   Community 3: private (rw)
      No trap recipient configured yet
   Community 4: public (ro)
      No trap recipient configured yet
   Community 5: common (ro)
      No trap recipient configured yet
   Community 6: FibreChannel (ro)
      No trap recipient configured yet
sw5:admin>
```

Figure A-12. agtcfgDefault command example

Table A-2
agtcfg Field Descriptions

Field	Description
sysDescr	The system description (in MIB-II definition). The default value is set as “Fibre Channel Switch.”
sysLocation	The location of the switch (in MIB-II). The default value is set as “End User Premise.”
sysContact	The contact information for this system (switch). The default value is set as “Field Support.”

continued

Table A-2
agtcfg Field Descriptions *continued*

Field	Description
swEventTrapLevel	The event trap level in conjunction with an event's severity level. When an event occurs with a severity level at or below the set value, the SNMP trap swEventTrap is sent to configured trap recipients. By default, this value is set at 0, implying that no swEventTrap is sent. Possible values are: ■ 0—None ■ 1—Critical ■ 2—Error ■ 3—Warning ■ 4—Informational ■ 5—Debug
authTraps	The authentication trap authenticationFailure is transmitted to configured trap recipients when the agent receives a protocol message that is not properly authenticated. In the context of SNMPv1 and SNMPv2c, this means that a request contains a community string that is not known to the agent. The default value for this parameter is 0 (disabled).

There are six communities and respective trap recipients supported by the agent. The first three communities are for read-write access (rw) and the last three are for read-only access (ro). The factory default value for the trap recipient of each community is 0.0.0.0. The factory default values for the community strings are:

1. Secret Code
2. OrigEquipMfr
3. private
4. public
5. common
6. FibreChannel

aliasShow

Figure A-13 shows the aliasShow command, which displays local Alias Server information. If there is no local alias group, a message stating that is displayed. The command fields are described in Table A-3.

```
admin> aliasShow
The Local Alias Server has 1 entry
Alias ID Creator Token [rb, type, grptype, qlfr] Member List
fffb01  fffffd  [40, 05, 10000060 69000015] {2d0113 2d0813}
```

Figure A-13. aliasShow command example

Table A-3
aliasShow Command Field Descriptions

Field	Description
Alias ID	The multicast address, which has the format of FFFBxx, where xx is an odd number starting at 01 and continuing through 239. This is the name of the multicast group.
Creator	The Fibre Channel address ID of the N_Port that created this alias group
Creator Token	The Alias Token provided to map to the alias group. The token consists of four subfields: ■ rb—Routing bits ■ type—Upper level application type ■ grptype—Alias group type ■ qlfr—Alias Qualifier of the group
Member List	A list of member address IDs

backSpace

Figure A-14 shows the backSpace command, which changes the backspace value used by the shell between the default value of hex 08, which translates to the standard **Backspace** key when using Windows NT and Windows 9x, and an alternate value of hex 7F, which translates to the standard **Delete** key when using Windows NT and Windows 9x. The parameter can be set to "0" or "1". When set to "0', the standard backspace character (BACKSPACE) is used. When set to "1', the alternate backspace character (DEL) is used. The operation may be different depending on the settings for the **Backspace** and **Delete** keys in your operating system configurations.

```
admin> backspace 0
Committing configuration…done.
BackSpace character is now BACKSPACE (hex 08)

admin> backspace 1
Committing configuration…done.
BackSpace character is now DEL (hex 7F)

admin> backspace
Committing configuration…done.
BackSpace character is DEL (hex 7F)
```

Figure A-14. backSpace command example

configure

Figure A-15 through Figure A-17 show the configure command, which is used to set some of the switch configuration parameters. This command cannot be executed on an enabled switch. Disable the switch by using the switchDisable command.

The configure command is navigated by entering a series of collapsible top-level menus. Each menu divides the various switch configuration parameters into logical groups, which include fabric parameters, virtual channel parameters, arbitrated loop parameters, and system service parameters. Each top-level menu and its associated submenus consist of a text prompt, a list of acceptable values, and the current value (shown in brackets). The current value is used in the absence of an entered value when a carriage return is the only input entered at the prompt.

```
switch:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no]
Virtual Channel parameters (yes, y, no, n): [no]
Arbitrated Loop parameters (yes, y, no, n): [no]
System services (yes, y, no, n): [no]
No changes.
```

Figure A-15. Top-level menus for the configure command

Entering out-of-range or inappropriate values causes error messages to display and the original entry prompt to redisplay. You can cancel the command at any time by sending an interrupt control character (**Ctrl+C**). You can also complete the command at any time, with the current changes saved, by sending an end-of-file control character (**Ctrl+D**).

```
switch:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] yes
Domain: (1..239) [1]
BB credit: (1..16) [16]
R_A_TOV: (4000..120000) [10000]
E_D_TOV: (1000..5000) [2000]
Data field size: (256..2112) [2112]
Non-SCSI Tachyon Mode: (0..1) [0]
Disable Device Probing: (0..1) [0]
Suppress Class F Traffic: (0..1) [0]
VC Encoded Address Mode: (0..1) [1]
Disable Transitive Mode: (0..1) [0]
Per-frame Route Priority: (0..1) [0]

Virtual Channel parameters (yes, y, no, n): [no] yes

VC Link Control: (0..1) [0]
VC Class 2: (2..5) [2]
VC Class 3: (2..5) [3]
VC Multicast: (6..7) [7]
VC Priority 2: (2..3) [2]
VC Priority 3: (2..3) [2]
VC Priority 4: (2..3) [2]
VC Priority 5: (2..3) [2]
VC Priority 6: (2..3) [3]
VC Priority 7: (2..3) [3]

Arbitrated Loop parameters (yes, y, no, n): [no] yes

Send FAN frames?: (0..1) [1]

Always Send RSCN: (0..1) [1]

Do Not Allow AL_PA 0x00

QuickLoop Soft Init?: (0..1) [0]

System services (yes, y, no, n): [no] yes

rstatd (on, off): [off] on
rusersd (on, off): [off] on
Disable RLS probing (on, off):[on]
No changes.
```

Figure A-16. Top-level menus and submenus for the configure command

```
switch:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] y
Domain: (1..239) [0] 256
integer must be between 1 and 239 - please re-enter
Domain: (1..239) [0]
BB credit: (1..16) [16] one
Input not acceptable, please re-enter
BB credit: (1..16) [16]
R_A_TOV: (4000..120000) [10000]
E_D_TOV: (1000..5000) [2000] 4900
integer must be a multiple of 1000 - please re-enter
E_D_TOV: (1000..5000) [2000] 5000
Data field size: (256..2112) [2112] ^D
Committing configuration...done.
```

Figure A-17. Configure command with inappropriate inputs

A number of parameters control the overall behavior of the fabric. Some of these values, such as the domain, are normally assigned automatically by the fabric and can be different from one switch to another in the fabric. Other parameters, such as the buffer-to-buffer credit or the time out values, can be changed to suit particular applications or operating environments but must be in agreement among all switches to allow the fabric to form. Table A-4 defines the settings affecting the fabric that can be changed.

Table A-4
Adjustable Fabric Settings

Field	Type	Default	Range
Domain	Number	1	Varies
BB Credit	Number	16	1 - 16
R_A_TOV	Number	10000	E_D_TOV * 2 to 120000
E_D_TOV	Number	2000	1000 to R_A_TOV / 2
Data Field Size	Number	2112	256 to 2112
Non-SCSI Tachyon Mode	Boolean	0	0 or 1
Disable Device Probing	Boolean	0	0 or 1
VC Encoded Address Mode	Boolean	0	0 or 1
Disable Translative Mode	Boolean	0	0 or 1
Per-frame Route Priority	Boolean	0	0 or 1

Table A-5 lists the configurable fabric parameters.

Table A-5
Fabric Parameters

Field	Description
Domain	The domain number identifies the switch in a fabric and can be any value between 1 and 239. Normally, this value is automatically assigned by the fabric.
BB Credit	The buffer-to-buffer (BB) credit represents the number of buffers, in a range from 1 to 16, available to the host. For a complete description of this value, refer to the industry specification Fibre Channel Physical and Signaling Interface (FC-PH).
R_A_TOV	The Resource Allocation Time Out Value (R_A_TOV) is displayed in milliseconds. This variable works with the variable E_D_TOV to determine the switch's actions when presented with an error condition. Allocated circuit resources with detected errors are not released until the time out value has expired. If the condition is resolved prior to the time out, the internal time out clock resets and waits for the next error condition.
E_D_TOV	The Error Detect Time Out Value (E_D_TOV) is displayed in milliseconds. This timer flags a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, then an error condition is met.
Data Field Size	The Data Field Size specifies the largest possible value, in bytes, for the size of a type 1 (data) frame. The switch advertises this value to other switches in the fabric during construction of the fabric as well as to other devices when they connect to the fabric. Setting this to a value smaller than 2112 can result in decreased performance.

continued

Table A-5
Fabric Parameters *continued*

Field	Description
Non-SCSI Tachyon Mode	When set, multiple sequences from different sources are interleaved to Tachyon-based controllers at sequence boundaries rather than at frame boundaries, resulting in better performance from Tachyon-based controllers. Set this mode when there are no Tachyon-based SCSI host adapters connected to the fabric.
Disable Device Probing	When device probing is disabled, devices that do not register themselves with the Name Server will not be present in the Name Server database. Set this mode only if the switch's N_Port discovery process (PLOGI, PRLI, INQUIRY) causes some attached device to fail.
VC Encoded Address Mode	When this mode is set, frame source and destination addresses use an address format compatible with first-generation switches. Set this mode only if the fabric includes such switches. In this mode, the maximum number of switches in a fabric is limited to 32.
Disable Translative Mode	This setting is only relevant if the VC Encoded Address Mode is also set. When set, this setting maintains explicit address compatibility with first-generation switches. However, enabling this feature also disables translative or phantom addressing. Set this mode only if hardware or software systems that explicitly rely on a specific frame address format are attached to the fabric.
Per-frame Route Priority	In addition to the eight virtual channels used in frame routing priority, support is also available for per-frame based prioritization. When set, the virtual channel ID will be used in conjunction with a frame header to form the final virtual channel ID.

The switch can be tuned for a specific application by configuring the parameters for the switch's eight virtual channels. The first two virtual channels are reserved for the switch's internal functions and are not user-configurable. The default virtual channel settings have already been optimized for switch performance. Changing the default values, if properly selected, can improve switch performance somewhat, but can also severely degrade switch performance. Do not change these settings without fully understanding the effects of those changes.

Table A-6
Virtual Channel Parameters

Field	Description	Default
VC Link Control	This changes the virtual channel used for N_Port-generated, Class 2 link control frames (ACKs, P_BSYs, and P_RJTs). 0—Forces N_Port-generated link control frames to be sent back using a Class 2 data virtual channel 1—Forces N_Port-generated link control frames to be sent back using a virtual channel normally reserved for fabric-internal traffic	0
VC Class 2	Sets the virtual channel used for class 2 frame traffic. Can be set to virtual channel 2, 3, 4, or 5.	2
VC Class 3	Sets the virtual channel used for class 3 frame traffic. Can be set to virtual channel 2, 3, 4, or 5.	3
VC Multicast	Sets the virtual channel used for multicast frame traffic. Verify that the multicast channel has the frame class priority set to the frame class of the expected traffic.	7
VC Priority 2-7	The numbers displayed show the priorities assigned to each of the switch's virtual channels. Allowed values are 2 or 3, indicating that the channel gives priority to either Class 2 or Class 3 frame traffic, respectively.	2 or 3

Table A-7
Arbitrated Loop Parameters and System Services

Field	Description	Default
Send FAN frames?	Fabric Address Notification (FAN) frames are sent by the fabric to notify public loop devices about their node ID and address. 0—No, do not send Fabric Address Notification frames. 1—Yes, send Fabric Address Notification frames.	1
Always send RSCN?	Following the completion of loop initialization, a remote state change notification (RSCN) is issued only when FL_Ports detect the presence of new devices or the absence of preexisting devices. When this feature is set, an RSCN will always be issued following the completion of loop initialization, regardless of the presence or absence of new or preexisting devices.	0
Do Not Allow AL_PA 0x00?	Prevents the FL_Port from using AL_PA 0x00. Set this parameter to 1 to force the FL_Port to go to the next available AL_PA upon initialization.	0
rstatd	Dynamically enables or disables a server that returns information via remote procedure calls (RPC) about system operation information. The protocol provides for a wide-range of system statistics; however, only the Ethernet interface statistics and system up time are supported. The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so on) the commands to retrieve the information are rup and rsysinfo. Refer to your local system documentation for the appropriate usage of the rup, rsysinfo, or equivalent commands.	Off
rusersd	Dynamically enables or disables a server that returns information via remote procedure calls (RPC) about the user logged in to the system. The information returned includes: the user login name, the system name, the login protocol or type, login time, idle time, and remote login location (if applicable). The retrieval of this information is supported by a number of operating systems that support RPC. On most UNIX-based systems (HP-UX, Irix, Linux, Solaris, and so on) the command to retrieve the information is rusers. Refer to your local system documentation for the appropriate usage of the rusers or equivalent command.	Off

configShow

The configShow command displays the current settings of many of the switch's configurable parameters. Figure A-18 shows the operation of the command. The output of the command is divided into two sections: the first displays the switch's boot settings and the second displays other configuration parameters, most of which are set from the configure command.

```
switch:admin> configShow
Ethernet address: 0:60:69:0:60:10
Nvram data: fei(0,0)host:/usr/switch/firmware e=192.168.1.2
g=192.168.1.254
u=user tn=switch
Type <CR> to continue, Q<CR> to stop:
diag.postDisable:
fabric.domain: 1
fabric.ops.BBCredit: 16
fabric.ops.E_D_TOV:2000
fabric.ops.R_A_TOV:10000
fabric.ops.dataFieldSize:2112
fabric.ops.mode.fcpProbeDisable:0
fabric.ops.mode.isolate:0
fabric.ops.mode.noClassF:0
fabric.ops.mode.tachyonCompat: 0
fabric.ops.mode.unicastOnly: 0
fabric.ops.mode.useCsCtl:0
fabric.ops.mode.vcEncode:0
fabric.ops.vc.class.2: 2
fabric.ops.vc.class.3: 3
fabric.ops.vc.config: 0xc0
fabric.ops.vc.linkCtrl: 0
fabric.ops.vc.multicast:7
fc4.fclp.address:0.0.0.0
fc4.fclp.mask: 0.0.0.0
fcAL.alwaysSendRSCN:1
fcAL.fanFrameDisable:0
fcAL.useAltBBCredit:0
lcdContrast:128
lcdContrast.orange:208
licenseKey:none
route.delayReroute:0
route.embeddedPortBcast:1
route.stickyRoutes:0
rpc.rstatd:0
rpc.rusersd:0
xlativeModeDisable:0
```

Figure A-18. configShow command example

configDefault

Figure A-19 shows the configDefault command, which resets some of the switch configuration values to their factory default values. This command also configures the switch to boot from its internal firmware if it has been previously configured to boot from the network. This command cannot be executed on an enabled switch; you must first disable the switch using the switchDisable command.

```
switch:admin> configDefault
Committing configuration...done.
```

Figure A-19. configDefault command example

Because the switch caches some configuration parameters, reboot the switch immediately following the execution of the configDefault command, otherwise unexpected behavior can result. With the exception of the following, all configuration parameters are reset to their default values:

- World Wide Name
- Ethernet MAC address
- Ethernet IP address and subnetmask
- IP gateway address
- SNMP configuration
- Zoning configuration
- License keys
- System name

configDownload

Figure A-20 shows the configDownload command. The Switch configuration file (including zoning) may be downloaded from a host using either FTP or RSHD.

```
switch:admin>configDownload
Server Name or IP Address [host]:
IP Address for Server:
IP Address for Server:
IP Address for Server:
User Name [user]:
File Name [config.txt]:
Protocol (RSHD or FTP) [rshd]:
```

Figure A-20. configDownload command example

configUpload

Figure A-21 shows the configUpload command. The Switch configuration file (including zoning) may be uploaded from a host using either FTP or RSHD.

```
switch:admin>configUpload
Server Name or IP Address [host]:
IP Address for Server:
User Name [user]:
File Name [config.txt]:
Protocol (RSHD or FTP) [rshd]:
```

Figure A-21. configUpload command example

date

Figure A-22 shows the date command, which displays the system date and time. To set the date and time:

1. Type the date command followed by the date in the format "mmddHHMMyy" where:
   - mm is the month
   - dd is the day
   - HH is the hour
   - MM is the minutes
   - yy is the year.

     The system is year 2000 compliant, where 00 through 69 equals 20xx and 70 through 99 equals 19xx.
2. Press **Enter** to set the date and time.

```
admin> date
Mon Jul  7 08:48:01 1997
value = 25 = 0x19
admin> date "060811241998"
Mon Jun 8 11:24:00 1998
```

Figure A-22. date command example

errDump

Figure A-23 shows the errDump command, which prints the contents of the error log with no page breaks.

```
switch:admin> errDump

Error 02
--------
0x103dc470 (tSilkworm): Apr 9 10:41:06
Error SENSOR-FAILED, 3, sensor 7 (Fan 2) is below minimum

Error 01
--------
0x103dc470 (tSilkworm): Apr 9 10:40:51
Error DIAG-TIMEOUT, 1,
Port 2 receive timeout.
```

Figure A-23. errDump command example

errShow

Figure A-24 shows the errShow command, which displays all detected errors. The error log stores the last 30 error types sensed by the switch. The log shows:

- Error number (01 to 30)
- Date and time the first occurrence of each error type was sensed
- Total number of occurrences of each error type (up to 999)
- Error type
- Error level for each error type:
  - 0–Panic (When this level is reached, the switch automatically reboots and the display no longer shows the error.)
  - 1–Critical
  - 2–Error
  - 3–Warning
  - 4–Debug

```
admin> errShow

Error 02
--------
0x103dc470 (tSilkworm): Apr  9 10:41:06
   Error SENSOR-FAILED, 3, sensor 7 (Fan 2) is below
minimum

Type <CR> to continue, Q<CR> to stop:

Error 01
--------
0x103dc470 (tSilkworm): Apr  9 10:40:51
   Error DIAG-TIMEOUT, 1,
  Port 2 receive timeout.

Type <CR> to continue, Q<CR> to stop:
```

Figure A-24. errShow command example

fabricShow

Figure A-25 shows the fabricShow command, which displays a list of switches and multicast alias groups in a fabric. If the switch supporting the Telnet connection does not have a Fabric Operating System license, this command only indicates that switch. Table A-8 describes the fields.

```
admin> fabricShow
Switch ID  Worldwide Name           Enet IP Addr    FC IP Addr  Name
-----------------------------------------------------------------------
0: fffc40  10:00:00:60:69:00:10:63  192.168.1.1     0.0.0.0      "sw1"
1: fffc41  10:00:00:60:69:00:0a:12  192.168.1.2     0.0.0.0      "sw2"
2: fffc42  10:00:00:60:69:00:01:b4  192.168.1.3     0.0.0.0     >"sw3"
```

Figure A-25. fabricShow command example

Table A-8
fabricShow Command Field Descriptions

Fabric Element	Description
switch n	Each line shows: ■ The switch's domain ID (0 - 31) ■ The switch's embedded port ID ■ The switch's World Wide Name ■ The switch's Ethernet and FC IP addresses ■ The switch's name (a greater than [>] symbol indicates the principle switch in the fabric)
multicast alias group	Each line shows: ■ The alias group number (0-30) ■ The alias group ID ■ The alias token Alias groups are only created on demand by requests to the alias server. Typically no groups are listed.

fakeModel

Figure A-26 shows the fakeModel command, which changes the view of the switch from the default model to an alternate model to ensure compatibility between new switch models and older versions of firmware within the same fabric. The command allows new switch models to be viewed as a similar but alternate model in the fabric window of Web Management Tools. This is only necessary in fabrics with mixed firmware, with some switches running firmware earlier than v2.1.

A similar alternate model should be used, for example, an 8-port model for an 8-port representation. When the switch is selected, the actual switch model is displayed, regardless of the fakeModel setting.

NOTE: This command is not included in the help list of commands.

Table A-9
Parameters

Value	Description
None	Current setting is displayed
0	Sets the switch to the actual model type
1	Sets the switch model to Fibre Channel SAN Switch 8-EL
2	Sets the switch model to Fibre Channel SAN Switch 16
3	Sets the switch model to Fibre Channel SAN Switch 8

```
admin> fakeModel
Fakemodel number is 1

admin> fakeModel 0
Committing configuration…done.
```

Figure A-26. fakeModel command example

fanShow

Figure A-27 shows the fanShow command, which displays the current status of the switch's fans. The format of the display varies according to the switch model and number of fans present. The status of each fan is shown as:

- OK—Fan is functioning correctly.
- Absent—Fan is not present.
- Below minimum—Fan is present but not rotating or rotating too slowly.

```
admin> fanShow
Fan 1 is OK, speed is 8460 RPM
Fan 2 is OK, speed is 8220 RPM
Fan 3 is OK, speed is 8340 RPM
Fan 4 is OK, speed is 8850 RPM
```

Figure A-27. fanShow command example

fastboot

Figure A-28 shows the fastboot command, which is a warm reboot that bypasses Power On Self-Test (POST) and takes about one minute to reboot the switch. The switch can be in any operational state (enabled or disabled) before rebooting.

```
admin> fastboot

Rebooting...
```

Figure A-28. fastboot command example

firmwareDownload

The firmwareDownload command downloads firmware into flash memory. This command can be executed on an operational switch. A reboot is required to initiate the new firmware after the download has completed.

Firmware can be downloaded from a Unix host, Windows 95 host, or Windows NT host. For a Unix host, no special software is needed. For Windows 95 or Windows NT, a daemon to support an RSH is required. Firmware is downloaded through an RCP command running on top of TCP between the switch and the host.

A Fibre Channel SAN Switch comes with preloaded firmware. In most cases there is no need to update the firmware on a new switch. The firmware version can be determined by using the front panel of a Fibre Channel SAN Switch 16 or by using a Telnet command.

To upgrade the firmware of a Fibre Channel SAN Switch, use the latest version of the Fibre Channel SAN Switch CD. Use one of the following three procedures (Windows NT Intel, Windows NT Alpha, or Tru64 Unix).

Host with Windows NT Intel

To load the firmware from a Compaq PC running Windows NT Intel:

1. Copy the files *Rshd.exe* and *Cat.exe* to the root directory for your system. These files are found in:
   D:\DSGGB\Firmware\NTIntel\Rshd.exe
   D:\DSGGB\Firmware\NTIntel\Cat.exe
   D:\DSGGB\Firmware\NTIntel\V2.1.7

   where D:\ is the drive letter for the CD and V2.1.7 is the latest version of firmware.

2. Double-click *Rshd.exe*. RSHD is a server program that allows the switch to request the firmware from the host over an Ethernet connection. Leave RSHD running in a separate window.

3. Click Start > Run and enter TELNET.

4. Click Connect > Remote System.

5. In the Host Name field, type the IP address of your Fibre Channel SAN Switch and click the Connect button.

6. Log in as:

   admin
   password: password

7. At the prompt, type:

   firmwareDownload "192.168.60.200", "administrator" , "v2.1.7"

   where "192.168.60.200" is the IP address of your host computer, "administrator" is the account you are using to run *Rshd.exe*, and "v2.1.7" is the firmware image to be downloaded to the switch.

   NOTE: *Rshd.exe* must be run from the directory that contains the *Cat.exe* file.

   The output displays as follows:

   1330320+203572+427356
   writing flash 0 .....
   writing flash 1 .....
   download complete
   switch:admin>

8. Click the RSHD window and click File > Exit.

9. Select the Telnet window and enter reboot. The switch reboots and copies the firmware into RAM.

Host with Windows NT Alpha

To load the firmware from a host running Windows NT Alpha:

1. Copy the files *Rshd.exe* and *Cat.exe* to the root directory for your system. These files can be found in:
   D:\DSGGB\Firmware\NTAlpha\Rshd.exe
   D:\DSGGB\Firmware\NTAlpha\Cat.exe
   D:\DSGGB\firmware\NTAlpha\V2.1.7

   where D:\ is the drive letter for the CD and V2.1.7 is the latest version of firmware.
2. Double-click *Rshd.exe*. RSHD is a server program that allows the switch to request the firmware from the host over an Ethernet connection. Leave RSHD running in a separate window.
3. Click Start > Run and enter TELNET.
4. Click Connect > Remote System.
5. In the Host Name field, type the IP address of your Fibre Channel SAN Switch and click the Connect button.
6. Log in as:

   admin
   password: password
7. At the prompt, type:

   firmwareDownload "192.168.60.200", "administrator" , "v2.1.7"

   where "192.168.60.200" is the IP address of your host computer, "administrator" is the account you are using to run *Rshd.exe*, and "v2.1.7" is the firmware image to be downloaded to the switch.

   NOTE: *Rshd.exe* must be run from the directory that contains the *Cat.exe* file.

   The output displays as follows:

   1330320+203572+427356
   writing flash 0 .....
   writing flash 1 .....
   download complete
   switch:admin>
8. Click the RSHD window and click File > Exit.
9. Select the Telnet window and enter reboot. The switch reboots and copies the firmware into RAM.

Host with Tru64 (Unix)

To load the firmware from a host running Compaq Tru64 (UNIX):

1. Mount the CD device by using the following command:

   mount -t cdfs -r /dev/rz5c /mnt

   where 5 is the unit number of your CD drive.

2. Change to the CD directory by entering:

   cd mnt

3. To copy the firmware to the host, enter the following command line:

   cp DSGGB/Firmware/V2.1.5/mary/tmp/V2.1.7

   where mary is the user name on the Tru64 host system and V2.1.7 is the firmware image to be downloaded to the switch.

   NOTE: The Fibre Channel SAN Switch uses the remote shell capabilities of UNIX to log in to the Tru64 UNIX host and copy the firmware image. The user (mary) and the switch's IP address must be in the *.rhosts* file on the Tru64 UNIX host to allow login without a password.

4. Telnet to the switch by entering:

   Telnet <switch_hostname>
   user: admin
   pswd: <password>

5. To download the firmware from the host system to the switch flash memory, enter the following command line at the <switch>:admin> prompt:

   firmwareDownload "16.140.32.60", "mary", "/tmp/V2.1.7"

   where "16.140.32.60" is the IP address of the host system with the firmware image, "mary" is the user to RSH, and "/tmp/v2.1.7" is the firmware image to be loaded into the switch flash ROM.

   NOTE:

   - The quote marks are very important in the firmwareDownload command line.
   - RSH without a password must be enabled for the user that RSH is executing under. To enable RSH without a password, add the switch IP name to ~<user>/.rhosts). The format of .rhosts is: hostname [user].

6. Enter reboot at the Telnet prompt. The switch reboots and copies the firmware into RAM.

h

Figure A-29 shows the h command, which displays the shell history of the previous 20 commands. The older commands are replaced by new commands. The shell history is similar to the Unix Korn shell history facility with a built-in line editor that allows previously typed commands to be edited.

NOTE: The shell history is reset by a reboot.

```
admin=> h
   11   date
   12   dateShow
   13   switchName
   14   date "0117130198"
   15   nsShow
   16   fabricShow
   17   portDisable 5
   18   portEnable 5
   19   portLogShow 100
   20   h
   21   portShow 5
   22   portStatsShow 5
   23   ipAddrShow
   24   diagShow
   25   switchDisable
   26   switchShow
   27   portLoopbackTest
   28   portShow 5
   29   diagShow
   30   switchEnable
```

Figure A-29. h command example

help

Figure A-30 and Figure A-31 show the help command, which displays a list of commands in alphabetical order. The command syntax to display detailed information about individual commands is help <command>.

NOTE: The help display changes depending on the login user level. Only commands that are available to the current user are displayed. This example shows the admin level commands. Commands for optionally licensed products only display if the appropriate license key is installed.

```
switch:admin> help
agtcfgSet                Set SNMP agent configuration
agtcfgShow               Print SNMP agent configuration
agtcfgDefault            reset SNMP agent to factory defaults
aliasShow                Print Alias Server information
backSpace                Set/clear alternate backspace character
configure                Set switch config parameters
configShow               Print switch config parameters
configDefault            Reset config to factory default
configDownload           Load switch config from a server
configUpload             Save switch config to a server
date                     Print/set the system date and time
errDump                  Print error log (no page breaks)
errShow                  Print error log
fabricShow               Print fabric membership info
fanShow                  Print fan status
fastboot                 Reboot this switch, bypassing POST
firmwareDownload         Download firmware into switch
h                        Print shell history
help                     Print this list
i                        Print task summary
ifModeSet                Set network link operating mode
ifModeShow               Print network link operating mode
ifShow                   Print network interface information
ipAddrSet                Set ethernet and FC IP addresses
ipAddrShow               Print ethernet and FC IP addresses
login                    Login as a new user
logout                   Logout from remote session
nsAllShow                Print global Name Server information
nsShow                   Print local Name Server information
passwd                   Set usernames and passwords
portCfgMcastLoopback     Configure multicast loopback port
portDisable              Disable a specified port
portEnable               Enable a specified port
portErrShow              Displays error summary for all ports
portLogClear             Clear port activity log
portLogDump              Print port log (no page breaks)
portLogShow              Print port activity log
portPerfShow             Print port throughput numbers
portShow                 Print state of specified port
portStatsShow            Print hardware statistics
psShow                   Print power supply status
reboot                   Reboot this switch
switchDisable            Disable this switch
switchEnable             Enable this switch
```

Figure A-30. help command example

```
switchName          Print/set this switch's name
switchShow          Print switch and port status
syslogdIp           Print/set syslog daemon IP address
tempShow            Print temperature readings
uptime              Print switch's operational time
version             Print firmware version
diagHelp            Print diagnostic help info
licenseHelp         Print licensing help info
qlHelp              Print quickloop help info
routeHelp           Print routing help info
zoneHelp            Print zoning help info
```

Figure A-31. help command example continued

i

Figure A-32 shows the i command, which displays a currently running task summary. Table A-10 describes the command fields.

```
admin>i
NAME       ENTRY          TID      PRI  STATUS    PC       SP       ERRNO  DELAY
------     -------        ------   ---  --------  ------   --------  ------  ----
tExcTask   excTask        103f7eb0 0      PEND     1014f718 103f8200 3d0001 0
tLogTask   _logTask       103f5f30 0      PEND     1014f718 103f6280 0      0
tShell     _shellTask     103c6e40 1      READY    101367c0 103c70b0 c0002  0
tRlogind   _rlogind       103ee0f0 2      PEND     101331e0 103ee7e0 0      0
tTelnetd   _telnetd       103ec160 2      PEND     101331e0 103ec5d0 0      0
tTelnetOutT _telnetOutTa  103711b0 2      READY    101331e0 103717b0 0      0
tTelnetInTa _telnetInTas  1036d330 2      READY    101330e4 1036d9b0 0      0
tTimers    _timerTask     103fbd80 10     PEND     1014f718 103fc100 0      0
tNetTask   _netTask       103f0370 50     READY    10134280 103f0740 0      0
tSwitch    _switchTask    103e9500 80     PEND+T   1014f718 103e9900 3d0004 36
tPBmenu    _menuTask      103d7c20 90     PEND     1014f718 103d7fe0 0      0
tReceive   _portRxTask    103d4450 100    PEND     1014f718 103d47d0 0      0
tTransmit  _portTxTask    103d2eb0 100    PEND     1014f718 103d3230 0      0
tFabric    _fabricTask    103b9530 100    PEND     1014f718 103b98f0 3d0004 0
tFspf      _fspfTask      103b7340 100    PEND     1014f718 103b76c0 0      0
tFcph      _fcphTask      103bde50 120    PEND+T   1014f718 103be1d0 3d0004 31
tZone      _cfgTask       10374ef0 130    PEND     1014f718 10375270 0      0
tFcp       _fcpTask       103bbd00 150    PEND+T   1014f718 103bc080 3d0004 773
tSnmpd     101394b0       103b3500 150    PEND     101331e0 103b4250 5b0002 0
tHttpD     _STARTUP_Web   103b1e70 150    PEND     101331e0 103b2330 0      0
tNSd       _ns_svr        103aca10 150    PEND     1014f718 103acda0 0      0
tASd       _as_svr        103812d0 150    PEND     1014f718 10381650 0      0
```

Figure A-32. i command example

Table A-10
i Command Field Descriptions

Field	Description
Name	Task name
Entry	Task entry point ID
TID	Task ID
PRI	Task priority with VxWorks
Status	■ READY—Task is not waiting for any resource other than the processor. ■ PEND—Task is blocked due to the unavailability of some resource. ■ DELAY—Task is asleep for some duration. ■ SUSPEND—Task is unavailable for execution, but not delayed or pending. ■ DELAY+S—Task is delayed and suspended. ■ PEND+S—Task is pending and suspended. ■ PEND+T—Task is pending with a timeout. ■ PEND+S+T—Task is pending with a timeout and suspended. ■ DEAD—Task no longer exists.
PC	Program counter
SP	Stack pointer
ERRNO	Last error number generated by this task
Delay	For pending tasks, the amount of time a task has been waiting to execute

ifModeSet

Figure A-33 shows the ifModeSet command, which sets the link operating mode for a network interface. The interface name is in quotes “interface”. The “interface” argument is of the form <name><physical-unit>, where <name> is the name of the network interface and <physical-unit> is the instance of that interface, for example “fei0”.

The network interfaces available on the system are listed with the ifShow command.

The command begins by prompting the current operating mode and continues prompting other possible operating modes until one has been selected or until all the possibilities have been displayed. An operating mode is confirmed with a “y” or “yes” at a prompt. If an operating mode is selected different from the current mode, the change is saved and the command exits.

Rebooting is required for the changes to take effect.

```
admin> ifModeSet “fei0”
Auto-negotiate (yes, y, no, n): [no]
100 Mbps/Full Duplex (yes, y, no, n): [no]
100 Mbps/Half Duplex (yes, y, no, n): [no]
10 Mbps/Full Duplex (yes, y, no, n): [no]
10 Mbps/Half Duplex (yes, y, no, n): [no] yes
```

Figure A-33. ifModeSet command example

NOTE: Changing the link mode is not supported for all network interfaces and not necessarily supported for all Ethernet network interfaces. This command is only functional for “fei” interfaces.

NOTE: Forcing the link to an operating mode not supported by the network equipment to which it is attached can result in an inability to communicate with the system by its Ethernet interface.

ifModeShow

Figure A-34 shows the ifModeShow command, which displays the link operating mode for a network interface. The interface name is in quotes “interface”. The “interface” argument is of the form <name><physical-unit>, where <name> is the name of the network interface and <physical-unit> is the instance of that interface, for example “fei0”.

The network interfaces available on the system are listed with the ifShow command.

```
admin> ifModeShow “fei0”
fei (unit number 0):
Link mode: Auto-negotiate
```

Figure A-34. ifModeShow command example

NOTE: The link operating mode is not changeable for all network interfaces and not necessarily changeable for all Ethernet network interfaces. For interfaces in which this is not supported, the output for the link mode is “Not applicable”.

ifShow

Figure A-35 shows the ifShow command, which displays network interface information. The display includes three sections organized by interface:

- ei—Ethernet 10/100BaseT port
- lo—loopback interface
- fc—Fibre Channel (This section is omitted if IP over Fibre Channel is not configured.)

```
admin> ifShow
ei (unit number 0):
   Flags: (0x63) UP BROADCAST ARP RUNNING
   Internet address: 192.168.64.146
   Broadcast address: 192.168.64.255
   Netmask 0xffffff00 Subnetmask 0xffffff00
   Ethernet address is 00:60:69:00:04:64
   Metric is 0
   Maximum Transfer Unit size is 1500
   2089 packets received; 156 packets sent
   0 input errors; 0 output errors
   3 collisions
lo (unit number 0):
   Flags: (0x69) UP LOOPBACK ARP RUNNING
   Internet address: 127.0.0.1
   Netmask 0xff000000 Subnetmask 0xff000000
   Metric is 0
   Maximum Transfer Unit size is 4096
   0 packets received; 0 packets sent
   0 input errors; 0 output errors
   0 collisions
```

Figure A-35. ifShow command example

ipAddrSet

Figure A-36 shows the ipAddrSet command, which sets the switch's Ethernet IP address, Ethernet subnetmask, Fibre Channel IP address, Fibre Channel subnetmask, and gateway address. Table A-11 describes the command fields.

```
admin> ipAddrSet
Ethernet IP Address [192.158.1.14]:
Ethernet Subnetmask [255.255.255.0]:
Fibre Channel IP Address [none]:
Fibre Channel Subnetmask [none]:
Gateway Address [192.158.1.1]:
```

Figure A-36. ipAddrSet command example

Table A-11
ipAddrSet Command Field Descriptions

Field	Description
Ethernet IP Address	The default IP address on a new switch is a temporary number. Enter a valid IP address.
Ethernet Subnetmask	The Ethernet subnetmask value. The default subnetmask value is none. See your network administrator for the appropriate subnetmask value.
Fibre Channel IP Address	The Fibre Channel IP address for the switch. Enter a valid IP address.
Fibre Channel Subnetmask	The Fibre Channel subnetmask for the switch. The default is none.
Gateway Address	The gateway address. The default gateway address on a new switch is none. Enter a valid gateway address if required.

ipAddrShow

Figure A-37 shows the ipAddrShow command, which displays the switch's IP addresses. The fields are described in Table A-12.

```
admin> ipAddrShow
Ethernet IP Address: 192.158.1.14
Ethernet Subnetmask: 255.255.255.0
Fibre Channel IP Address: none
Fibre Channel Subnetmask: none
Gateway Address: 192.158.1.1
```

Figure A-37. ipAddrShow command example

login

Figure A-38 shows the login command, which logs in a user from a remote host. If a user is already logged in, the command logs out the user and lets a new user log in.

```
switch:user> login
login:admin
Password:
switch:admin>
```

Figure A-38. login command example

logout

Figure A-39 shows the logout command, which logs a user out from a remote session.

```
admin> logout
Connection closed.
```

Figure A-39. logout command example

nsAllShow

Figure A-40 shows the nsAllShow command, which displays a list of port IDs connected to the fabric. The nsAllShow command optionally takes an integer parameter, the value of the FC-PH type. For example, nsAllShow 8 shows all SCSI-FCP nodes. If the parameter is not provided, then Nx_Ports displays. This command only returns relevant data for switches that have a Fabric Operating System license.

```
admin> nsAllShow
2 Nx_Ports in the Fabric {
   614001 614301
}
value = 0 = 0x0

admin> nsAllShow 8
2 FCP Ports {
   6042ef 6045e8
}
```

Figure A-40. nsAllShow command example

nsShow

Figure A-41 shows the nsShow command, which displays the local name server information, including information about devices connected to the switch and cached information about devices connected to other switches in the fabric. The nsAllShow command shows information about all switches.

The message "There is no entry in the Local Name Server" displays if there is no information about the local switch. If information about the local switch is available, the number of name service entries displays.

```
admin> nsShow
The Local Name Server has 2 entries {
Type  Pid     COS     PortName      NodeName                 TTL(sec)
NL    614001; 3;00:00:00:00:00:00:00:00;00:00:00:00:00:00:00:00; na
NL    614301; 3;00:00:00:00:00:00:00:00;00:00:00:00:00:00:00:00; na
}
```

Figure A-41. nsShow command example

Table A-12
nsShow Command Field Descriptions

Field	Description
Type	The port type with one of the following values: ■ N—Indicates that this is an N_Port. ■ NL—Indicates that this is an NL_Port.
Pid	The address ID of the port in hexadecimal format
COS	The class of service supported by the port
PortName	The port WWN
NodeName	The node WWN associated with the port
TTL	The time-to-live value of the entry. This field is typically set to not applicable (na) for a local entry. An entry can be a cached version of a remote port, that is, not directly connected to this switch. In that case, the value equals the number of seconds before the cached entry expires and is deleted from the local database. A cached entry is marked with an asterisk (*).

passwd

Figure A-42 shows the passwd command, which sets usernames and passwords.

```
admin> passwd

username 1 [admin]:
"admin" password:
username 2 [user]:
"user" password:
username 3 [other]:
"other" password:
```

Figure A-42. passwd command example

The command syntax is passwd ["user name"]. The optional parameter <username> is a valid user name enclosed by quote marks.

> **NOTE:** If the current password is incorrect, the command exits without saving any changes. If the number of attempts to connect is exceeded, the command either steps to the next user or exits without saving any changes.

Special Inputs

The passwd command accepts the following inputs at the Telnet prompt.

- **Enter**—Accepts the default value (if applicable) and moves to the next prompt.
- **Ctrl+C**—Aborts the passwd command immediately and ignores all changes made.
- **Ctrl+D**—Terminates the passwd command and writes all changes to flash memory when entered alone at a prompt without any preceding input.

Examples

The following is a list of the passwd command's input and output examples. Only passwords at the current level and below can be changed.

1. Invalid user name.

```
admin> passwd "nobody"
passwd: nobody is not a valid user name.
```

2. Invalid command usage.

```
admin> passwd ""
Usage: passwd [username]
```

3. Permission denied.

```
admin> passwd "root"
passwd: Permission denied.
```

4. Change the user name.

```
admin> passwd "admin"
New username [admin]: maint
Old password:
passwd: Password unchanged.

Updating flash...done.
```

5. Change the user name and password.

```
maint> passwd "maint"
New username [maint]: admin
Old password:
New password:
Re-enter new password:
Updating flash...done.
```

6. Skip through the prompts without changes.

```
admin> passwd
New username [admin]:
Old password:
passwd: Password unchanged.
New username [user]:
Old password:
passwd: Password unchanged.
New username [other]:
Old password:
passwd: Password unchanged.
```

7. Surpass failure limit, then cancel the command.

```
admin> passwd
New username [admin]:
Old password:
New password:
Re-enter new password:
passwd: Passwords do not match; try again.
New password:
Re-enter new password:
passwd: Passwords do not match; try again.
New password:
Re-enter new password:
passwd: Number of failure attempts exceeded.
New username [user]: ^C
```

8. Change the user name and then finish with **Ctrl+D**.

```
admin> passwd
New username [admin]: maint
Old password: ^D
Updating flash...done.
maint>
```

portCfgMcastLoopback

Figure A-43 shows the portCfgMcastLoopback command, allows a user to dedicate an unused port in a leaf (edge) switch with no F_Port belonging to a multicast group, receive multicast frames.

When multicast frames are received at an edge switch with no member port, traffic will throttle down in the kilobytes per second (KB/s) range as embedded processor intervention is required to process it. However, when a port is assigned as the multicast loopback port, frames destined for any multicast group will be routed to that multicast loopback port where it is loopbacked to the port's receiver, which is turned off. This effectively sends the frames to a black hole. Since an embedded processor is not involved, traffic moves at normal (and full) speed.

Executing this command on a branch (middle) switch will not affect traffic. It can be configured for future use as an edge switch. The disadvantage is that the port cannot be used to connect to other devices.

The configuration is saved in the non-volatile memory and is persistent across switch reboot or power cycle.

The user will be prompted if:

- The selected port is already in use as an E_Port, or Fx_port
- Other ports are already configured as multicast loopbacks
- When a port is configured as a multicast loopback port:
  - Its port LED will blink a slow green indicating a loopback state. Its laser, if optical GBIC, will be disabled. It will not respond to any attempt to connect it to any device.
  - The comment field of switchShow will show that it is looped back to itself, for example:

    "port 3: sw No_Light Loopback→3"
  - The portFlags line of portShow will display the "F_PORT" and "INT_LB" flags, for example:

    "portFlags: 0x20249 PRESENT F_PORT U_PORT INT_LB LED"
  - mcastShow will show the port as a member in its "Member Ports" column.

The command syntax is portCfgMcastLoopback <port #, mode>. The "port #" parameter can be configured 0-7 or 0-15. The "mode" parameter is either "0" or "1". "0" means that the "port #" will be dedicated as a multicast loopback port. "1" means that the "port #" will be de-configured from its previous role as a multicast loopback port.

```
admin> portCfgMcastLoopback 3, 1
Committing configuration…done.
```

Figure A-43. portCfgMcastLoopback command example

portDisable

Figure A-44 shows the portDisable command, which disables a specified port. Devices attached to a disabled port cannot communicate with the fabric. The command syntax is portDisable <port #>.

```
admin> portDisable 2
```

Figure A-44. portDisable command example

NOTE: Unlike inserting a GBIC module into an interface card, portDisable and portEnable do not generate SNMP traps.

portEnable

Figure A-45 shows the portEnable command, which enables a specified port. The command syntax is portEnable <port #>.

```
admin> portEnable 2
```

Figure A-45. portEnable command example

portErrShow

Figure A-46 shows the portErrShow command, which displays an error summary for all ports. One output line displays per port, and shows error counters in ones, thousands (the number is followed by "k"), or millions (the number is followed by "m"). This example shows an eight-port switch, where port 6 has a high number of errors. The command fields are described in the following table.

```
switch:admin> portErrShow
   frames      enc  crc  too  too  bad  enc  disc  link  loss  loss  frjt  fbsy
     tx    rx   in  err  shrt long eof  out  c3    fail  sync  sig
  ----------------------------------------------------------------------------
0: 0     0    0   0    0    0    0    0    0     0     0     1     0     0
1: 2.5m  38   0   0    0    0    0    2    0     0     1     1     0     0
2: 0     0    0   0    0    0    0    0    0     0     0     1     0     0
3: 95k   15k  0   0    0    0    0    3    0     0     1     0     0     0
4: 0     0    0   0    0    0    0    0    0     0     0     1     0     0
5: 0     0    0   0    0    0    0    0    0     0     0     1     0     0
6: 61k   48   2   15   0    0    0    3k   0     0     2     0     0     0
7: 0     0    0   0    0    0    0    0    0     0     0     1     0     0
```

Figure A-46. portErrShow command example

Table A-13
portErrShow Command Field Descriptions

Field	Description
frames tx	Frames transmitted
frames rx	Frames received
enc in	Encoding errors inside of frames
crc err	Frames with CRC errors
too shrt	Frames shorter than minimum

continued

Table A-13
portErrShow Command Field Descriptions *continued*

Field	Description
too long	Frames longer than maximum
bad eof	Frames with bad end-of-frame delimiters
enc out	Encoding error outside of frames
disc c3	Class 3 frames discarded
link fail	Link failures (LF1 or LF2 states)
loss sync	Loss of synchronization
loss sig	Loss of signal
frjt	Frames rejected with F_RJT
fbsy	Frames busied with F_BSY

Note: Non-zero values in the portErrShow command fields do not indicate a bad switch. It is normal to have errors when connecting cables and powering up devices that are connected to the switch.

portLogClear

Figure A-47 shows the portLogClear command, which clears the data from the port log. The command syntax is portLogClear.

```
admin> portLogClear
```

Figure A-47. portLogClear command example

portLogDump

Figure A-48 shows the portLogDump command, which displays the port log without page breaks. The portLogDump and portLogShow commands are the same except for how much information the port log displays without intervention.

```
admin> portLogDump
time                    task     event    port  cmd      args
------                  ------   ------   ----- -----    ------
May 18 21:35:21.000 tSwitch  create                  tTimers
May 18 21:35:22.383 tSwitch  create                  tPBmenu
May 18 21:35:22.383 tSwitch  create                  tReceive
May 18 21:35:22.383 tSwitch  create                  tTransmit
May 18 21:35:22.383 tSwitch  start                   100
May 18 21:35:22.633 tSwitch  pstate   4     OL1
May 18 21:35:22.633 tSwitch  pstate   5     OL1
May 18 21:35:22.633 tSwitch  pstate   6     OL1
May 18 21:35:22.633 tSwitch  pstate   7     OL1
May 18 21:35:38.066 tSwitch  Tx3      3     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.083 tReceive Rx3      3     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.083 tSwitch  ioctl    3     80       a,0
May 18 21:35:38.083 tSwitch  Tx3      5     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.083 tReceive Rx3      5     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.083 tSwitch  ioctl    5     80       a,0
May 18 21:35:38.083 tSwitch  Tx3      7     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.099 tReceive Rx3      7     2112     02ffffd,00ffffd,4723bcbc
May 18 21:35:38.099 tSwitch  ioctl    7     80       a,0
May 18 21:35:41.049 tSwitch  disable  0               2
May 18 21:35:41.083 tSwitch  pstate   2     OL1
May 18 21:35:41.583 tSwitch  start                   0
May 18 21:35:41.599 tSwitch  pstate   0     LF2
May 18 21:35:41.599 tSwitch  pstate   2     OL1
May 18 21:35:41.599 tSwitch  pstate   3     LF2
May 18 21:35:54.216 tSwitch  enable   16              0
May 18 21:35:55.266 tSwitch  errlog   3     FANS-1_FAILED
```

Figure A-48. portLogDump command example

portLogShow

Figure A-49 shows the portLogShow command, which displays the switch's port activity. Entries consist of fabric login (link service request to a fabric F_Port 22fffffe), port login (link service request to the management server 22ffffa), and an inquiry request (unsolicited command to the management server 06ffffa). The entries are like the initial handshake between an F_Port and the Host Bus Adapter. Table A-14 describes the command fields.

```
admin> portLogShow
time                    task       event  port  cmd   args
-----                   -----      -----  ----  -----  -----
Jun 15 16:00:21.899  tReceive   pstate  2     OL2
Jun 15 16:00:21.899  tReceive   pstate  2     LR3
Jun 15 16:00:21.899  tReceive   pstate  2     AC
Jun 15 16:00:21.899  interrupt  scn     2     2
Jun 15 16:00:21.899  interrupt  scn     2     1
Jun 15 16:00:21.899  tFspf      ioctl   2     ab    ffffff,16
Jun 15 16:00:21.899  tFspf      ioctl   16    ab    ffffff,2
Jun 15 16:00:21.899  tReceive   Rx3     2     116   22fffffe, 00000000, 04000000
Jun 15 16:00:21.899  tReceive   ioctl   2     a2    210213,2
Jun 15 16:00:21.899  tReceive   scn     2     6
Jun 15 16:00:21.899  tFspf      ioctl   2     ac    0,0
Jun 15 16:00:21.899  tFspf      ioctl   2     aa    ffffff,16
Jun 15 16:00:21.899  tFspf      ioctl   16    aa    ffffff,2
Jun 15 16:00:21.899  tFspf      ioctl   2     ad    0,0
Jun 15 16:00:21.899  tFspf      Tx3     2     116   23210213, 00fffffe, 02000000
Jun 15 16:00:21.899  tReceive   Rx3     2     116   22ffffa, 00210213, 03000000
Jun 15 16:00:21.899  tSwitch    Tx3     2     116   23210213, 00ffffa, 02000000
Jun 15 16:00:21.899  tFcp       Tx3     2     116   22210213, 00fffc41, 03000000
Jun 15 16:00:21.899  tReceive   Rx3     2     32    06ffffa, 00210213, 00000000
Jun 15 16:00:21.899  tFcp       Tx3     2     36    01210213, 00ffffa, 0d000302
Jun 15 16:00:21.899  tFcp       Tx3     2     24    07210213, 00ffffa, 00000000
```

Figure A-49. portLogShow command example

Table A-14
portLogShow Command Field Descriptions

Field	Description
Time	The event's date and time in milliseconds.
Task	The task name that logged the event, or "interrupt" if the event was recorded from interrupt level code.
Event	The possible switch events include: ■ start—The switch starts running. ■ disable—A port is disabled. ■ enable—A port is enabled. ■ ioctl—A port I/O control is executed. ■ Tx—A frame is transmitted using class x. ■ Rx—A frame is received using class x. ■ scn—A state change notification is posted. ■ pstate—A port changes physical state. ■ ctin—A CT-based request is received (name server request). ■ ctout—A CT-based response is transmitted (name server request).
Port	Either the port number of the affected port or the last byte of a well-known address (for example, fc for the well-known Name Server address).

continued

Table A-14
portLogShow Command Field Descriptions *continued*

Field	Description
cmd	The cmd field represents different values depending on the task and event. The following definitions are included: ■ For ioctl events, cmd is the I/O control command code. ■ For Tx and Rx events, cmd is the payload size. ■ For scn events, cmd is the new state. ■ For pstate events, cmd is the new physical state. ■ For ctin events, cmd consists of two 2-byte subfields. ■ For ctout events, cmd consists of two 2-byte subfields.
pstate	For pstate events, the cmd field entries in upper case are Fibre Channel ANSI Standard (PC-PH) as follows: ■ AC—Active State ■ LR1—Link Reset: LR Transmit State ■ LR2—Link Reset: LR Receive State ■ LR3—Link Reset: LRR Receive State ■ LF1—Link Failure: NOS Transmit State ■ LF2—Link Failure: NOS Receive State ■ OL1—Offline: OLS Transmit State ■ OL2—Offline: OLS Receive State ■ OL3—Offline: Wait for OLS State

continued

Table A-14
portLogShow Command Field Descriptions *continued*

Field	Description
ioctl	For ioctl events, the cmd field entries in lower case are switch-specific as follows: ■ a1—Port is an E_Port ■ a2—Port is an F_Port ■ a3—Port is segmented ■ a4—Domain name is known ■ a5—Port enable ■ a6—Port disable ■ a7—Link reset ■ a8—Add unicast route ■ a9—Delete unicast route ■ aa—Add multicast route ■ ab—Delete multicast route ■ ac—Unicast routing table done ■ ad—Multicast routing table done ■ ae—Add a phantom device ■ af—Remove a phantom device For a ctin event, the first subfield indicates whether “argument 1” and “argument 2” would be valid: ■ 0000—no argument 1 and 2 ■ 0001—argument 1 is valid ■ 0003—arguments 1 and 2 are valid For ctout event, the cmd field consists of two 2-byte subfields, similar to ctin. The second subfield should contain a CT command code indicating an accept or reject: ■ 8001—reject ■ 8002—accept

continued

Table A-14
portLogShow Command Field Descriptions *continued*

Field	Description
args	The args field represents different values depending on the task and event. The following definitions are included: ■ For ioctl events, the I/O controls arguments. ■ For Tx and Rx events, the first two header words and the first payload word. ■ For ctin events, the args field generally represents the first and second words of the CT payload where they are valid. When there is an IPv4 address involved, this field shows the value of the IPv4 address, which is neither the first nor second word of the CT payload. ■ For ctout events, if the event is associated with an accept, then the args field generally represents the first and second words of the CT payload. When there is an IPv4 address involved, this field shows the value of the IPv4 address, which is neither the first nor second word of the CT payload. ■ If the event is associated with a rejection, the args field contains the reason for the rejection and an explanation code.
loopscn	For loopscn events: ■ OLP—Offline (disconnected or nonparticipating) ■ LIP—LIP sent (if the next argument is 8xxx) or received (if the next argument contains the lower two bytes of the LIP Primitive Sequence received), port entered OPEN-INIT state. ■ LIM—FL_Port is elected as LIM. ■ BMP—AL_PA bitmap is collected by the FL_Port. ■ ERR—An error occurred during the loopinit process, such as a loss of sync. ■ OLD—Port entered OLD_PORT state. ■ TMO—Loopinit timed out.

portPerfShow

Figure A-50 shows the portPerfShow command, which displays the throughput for all ports. The output is terminated by pressing **Enter** or **Ctrl+C**. The throughput number represents the number of bytes received plus the number of bytes transmitted and displays as bytes per second (B/s). Throughput numbers are shown either as B/s, KB/s, or megabytes per second (MB/s). This information is used to monitor port performance. One line per second is printed summarizing the traffic on all ports.

```
admin> portPerfShow
0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```

Figure A-50. portPerfShow command example

portShow

Figure A-51 shows the portShow command, which displays a summary of all ports. The fields are described in the following table. The command syntax is portShow <port #>.

```
admin> portShow 2
portFlags: 0x20021          PRESENT L_PORT LED
portType:  2.2
portState: 2        Offline
portPhys:  4        No_Light
portScn:   0
portRegs:  0xa0008000
portData:  0x103ce320
portId:    614200
portWwn:   20:02:00:60:69:00:04:64

Interrupts:    0        Link_failure:  0        Frjt:    0
Unknown:       0        Loss_of_sync:  0        Fbsy:    0
Lli:           0        Loss_of_sig:   0
Proc_rqrd:     0        Protocol_err:  0
Timed_out:     0        Invalid_word:  0
Rx_flushed:    0        Invalid_crc:   0
Tx_unavail:    0        Delim_err:     0
Free_buffer:   0        Address_err:   0
Overrun:       0        Lr_in:         0
Suspended:     0        Lr_out:        0
Parity_err:    0        Ols_in:        0
                        Ols_out:       0
```

Figure A-51. portShow command example

Table A-15
portShow Command Field Descriptions

Type	Field	Description
Port Definition	portFlags	The bitmap port status
	portType	The port type (G_port or FL_Port)
	portState	The port SNMP state; values include Online or Offline
	portPhys	The port physical state
	portScn	The port LED state*
	portRegs	Pointer of hardware register
	portData	Pointer to driver private data
	portId	The port address ID
	portWwn	The port World Wide Name

continued

Table A-15
portShow Command Field Descriptions *continued*

Type	Field	Description
Interrupt Statistics	Interrupts	Total number of interrupts
	Unknown	Number of unknown interrupts
	Lli	Number of low level interface (LLI) interrupts
	Proc_rqrd	Number of interrupts with processing (CPU) required
	Timed_out	Number of timed out interrupts
	Rx_flushed	Number of flushed transmissions
	Tx_unavail	Number of interrupted transmissions
	Free_buffer	Number of buffer interrupts
	Overrun	Number of buffer overruns
	Suspended	Number of suspended interrupts
	Parity_err	Number of parity errors
Error Statistics	Link_failure	Number of link failures
	Loss_of_sync	Loss of synchronization
	Loss_of_sig	Loss of signal (no light)
	Protocol_err	Protocol error
	Invalid_word	Invalid word (encoding errors inside of frames)
	Invalid_crc	Invalid CRC in a frame
	Delim_err	Delimiter error (order set)
	Address_err	Address ID error (S_ID D_ID)
	Lr_in	Link reset in (primitive sequence), does not apply to FL_Port
	Lr_out	Link reset out (primitive sequence), does not apply to FL_Port
	Ols_in	Offline resent in (primitive sequence), does not apply to FL_Port
	Ols_out	Offline resent in (primitive sequence), does not apply to FL_Port
	Frjt	Number of frames rejected
	Fbsy	Number of frames busy

NOTE: All port topologies except for E_port shows F_port for this field, as this is the logical state of the port. For example, a L_port in switchShow is a FL_port, thus logically a F_port.

portStatsShow

Figure A-52 shows the portStatsShow command. When used with a port number, this command gives a static view of port status. For example, to update the command and check if an error count is increasing, reissue the portStatsShow command to capture another snapshot. The command syntax is portStatsShow <port #>.

```
switch:admin> portStatsShow 2
stat_wtx          1379589     4-byte words transmitted
stat_wrx          473913      4-byte words received
stat_ftx          114957      Frames transmitted
stat_frx          40          Frames received
stat_c2_frx       0           Class 2 frames received
stat_c3_frx       34          Class 3 frames received
stat_lc_rx        3           Link control frames received
stat_mc_rx        0           Multicast frames received
stat_mc_to        0           Multicast timeouts
stat_mc_tx        0           Multicast frames transmitted
tim_rdy_pri       599970      Time R_RDY high priority
tim_txcrd_z       0           Time BB_credit zero
er_enc_in         0           Encoding errors inside of frames
er_crc            0           Frames with CRC errors
er_trunc          0           Frames shorter than minimum
er_toolong        0           Frames longer than maximum
er_bad_eof        0           Frames with bad end-of-frame
er_enc_out        74670       Encoding error outside of frames
er_disc_c3        0           Class 3 frames discarded
open              0           loop_open
transfer          0           loop_transfer
opened            0           FL_Port opened
starve_stop       0           tenancies stopped due to starvation
fl_tenancy        0           number of times FL has the tenancy
nl_tenancy        0           number of times NL has the tenancy
frame_nozone      0           frames rejected due to zone protection
```

Figure A-52. portStatsShow command example

Table A-16
portStatsShow Command Field Descriptions

Field	Description
stat_wtx	Number of 4-byte words transmitted from the port.
stat_wrx	Number of 4-byte words received by the port.
stat_ftx	Number of frames transmitted from the port.
stat_frx	Number of frames received by the port.
stat_c2_frx	Number of Class 2 frames received.
stat_c3_frx	Number of Class 3 frames received.
stat_lc_rx	Number of link control frames received.
stat_mc_rx	Number of multicast frames received.
stat_mc_to	Number of timeouts reported for multicast frames. A single frame could cause this counter to increment if it timed out for each multiple destination.
stat_mc_tx	Number of multicast frames transmitted.
tim_rdy_pri	Amount of time (measured in proprietary ticks) that R_RDY transmission has higher priority than frame transmission.
tim_txcrd_z	Time that this port cannot transmit frames due to a transmit buffer-to-buffer credit of zero.
er_enc_in	Received data: The number of 8b/10b encoding errors that have occurred inside frame boundaries. This counter is generally a nonzero value, although occasional errors can occur on a normal link and give a zero result. (Minimum compliance with the link bit error rate specification on a link continuously receiving frames would cause approximately one error every 20 minutes.)
er_crc	Received frames: The number of CRC errors detected.
er_trunc	Received frames: The number of frames that were shorter than the minimum Fibre Channel frame size (such as a header with no payload).
er_toolong	Received frames: The number of frames that were longer than the maximum Fibre Channel frame size (such as a header with a 2,112-byte payload).
er_bad_eof	The number of frames received with a badly formed end-of-frame.

continued

Table A-16
portStatsShow Command Field Descriptions *continued*

Field	Description
er_enc_out	Receive link: The number of 8b/10b encoding errors recorded outside frame boundaries. This number can become nonzero during link initialization but indicates a problem if it increments faster than the allowed link-bit error rate (approximately once every 20 minutes).
er_disc_c3	Receive link: The number of Class 3 frames discarded. Class 3 frames can be discarded due to timeouts or invalid/unreachable destinations. This quantity could increment at times during normal operation but might be used for diagnosing problems in some situations.
open	Loop_open: the number of times FL_Port entered the OPEN state.
transfer	Loop_transfer: the number of times FL_Port entered the TRANSFER state.
opened	FL_Port opened: the number of times FL_Port entered the OPENED state.
starve_stop	Loop tenancies stopped due to starvation.
fl_tenancy	Number of times FL_Port has the loop tenancy.
nl_tenancy	Number of times NL_Port has the loop tenancy.
frame_nozone	Number of frames rejected due to zone protection.

psShow

Figure A-53 shows the psShow command, which displays power supply status information. The format of the display varies according to the switch model and number of power supplies present. Possible values are:

- OK—The power supply is present and functioning correctly.
- Absent—The power supply is not present.
- Faulty—The power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

After the status line, power supply information displays including manufacture date, part number, serial number, and other information.

```
switch:admin> psShow
Power Supply 1 is OK
9835,DH000000208,60-0000734-01, A,00001, E108302A,01, 803350
Power Supply 2 is OK
9839,DH000000253,60-0000734-01, A,00001, E108302A,01, 803522
```

Figure A-53. psShow command example

NOTE: Status information is not available on certain Fibre Channel SAN Switches.

reboot

Figure A-54 shows the reboot command, which reboots the switch to the stored configuration in flash memory. The reboot lasts about 1½ minutes. The switch can be in any operational state (enabled or disabled) before rebooting.

```
admin> reboot
Rebooting...
```

Figure A-54. reboot command example

switchDisable

Figure A-55 shows the switchDisable command, which is used for diagnostic tests, maintenance functions, or replacement of a faulty switch. You can observe this process by watching the front panel LEDs change color from green to amber as each port inactivates.

```
admin> switchDisable
```

Figure A-55. switchDisable command example

switchEnable

The switchEnable command enables the switch and provides fabric information. You need to enable the switch after maintenance and diagnostic tests. In Figure A-56, the switch is enabled with a domain ID of 1. After the fabric is reconfigured, this switch is the principal address manager, capable of assigning domain IDs to other switches in the same fabric. You can observe this process by watching the front panel LEDs change color from green to amber as each port activates.

```
admin> switchEnable
value = 0 = 0x0
10  9  8  7  6  5  4  3  2  1
fabric: Principal switch
fabric: Domain 1
```

Figure A-56. switchEnable command example

NOTE: When a switch is powered on, it is automatically enabled.

switchName

Figure A-57 shows the switchName command, which displays or sets the switch's name. If a new name is specified and enclosed in quotes, the command sets the switch to that name. The command syntax is switchName <"name-of-switch">. If no new name is included, the command displays the switch's default name.

```
admin> switchName "sw3"

sw3
```

Figure A-57. switchName command example

Certain restrictions apply to the length and format of the switch name. Specifically, the name of the switch:

- Cannot exceed 19 characters in length
- Cannot contain characters other than upper or lower case letters (a-z), the numbers 0-9, or the underscore character (_)
- Must start with an upper or lower case letter (a-z)

NOTE: Switch names should be unique in a cascaded environment.

switchShow

Figure A-58 shows the switchShow command, which displays the switch and port status. The fields are described in the following table.

```
admin> switchShow
switchName:     open146
switchType:     3.1
switchState:    Online
switchRole:     Principal
switchDomain:   1
switchId:       fffc41
switchWwn:      10:00:00:60:69:00:04:64
port  0: sw    Online       L-Port  1 private, 1 phantom
port  1: --    No_Module    L-Port
port  2: sw    No_Light     L-Port
port  3: sw    Online       L-Port  1 private, 1 phantom
port  4: --    No_Module
port  5: sw    Online       E-Port  10:00:00:60:69:00:00:12 "sw1"(upstream)
port  6: sw    No_Light
port  7: sw    No_Light
port  8: sw    No_Light
port  9: sw    Online       E-Port  10:00:00:60:69:00:01:b4 "sw3"(downstream)
port 10: sw  No_Light
port 11: sw  No_Light
port 12: sw  No_Light
port 13: sw  No_Light
port 14: sw  No_Light
port 15: sw  No_Light
```

Figure A-58. switchShow command example

Table A-17
switchShow Command Field Descriptions

Field	Description
switchName	The switch name
switchType	The switch model and motherboard revision level
switchState	The state of this switch: online, offline, testing, or faulty.
switchRole	There are three possibilities for switchRole: ■ Master: The principal switch, as defined in FC-SW. ■ Slave: The switch is enabled and not the principal switch. ■ Disabled: The switch is disabled.
switchDomain	The domain ID of this switch can range from 0 to 31. The lowest domain numbered switch in a fabric will become the master.
switchID	The domain ID of this switch's embedded port is hex fffc00 to fffc7f.
switchWwn	The World Wide Name (WWN) of this switch, which is a unique identifier for each switch assigned by the manufacturer. A numbering scheme administered globally ensures that the WWN is unique for each switch.
Port Number	One line per port is printed after the switch summary. Each line shows the port number (0 to 15), the GBIC type, the port state, and a comment field.
GBIC type	The GBIC type follows the port number. The three GBIC types include: ■ -- no GBIC present ■ sw shortwave GBIC ■ lw longwave GBIC

continued

Table A-17
switchShow Command Field Descriptions *continued*

Field	Description
Port state	The port state follows the GBIC type. The possible port states include: ■ No_Card—No card is present in this switch slot. ■ No_Module—No GBIC module is in this port. ■ No_Light—The module is not receiving light. ■ No_Sync—The module is receiving light but it is out of sync. ■ In_Sync—The module is receiving light and it is in sync. ■ Laser_Flt—The module is signaling a laser fault (defective GBIC). ■ Port_Flt—The port has been marked faulty (defective GBIC, cable, or device). ■ Diag_Flt—The port failed diagnostics (defective G_Port or FL_Port card or motherboard). ■ Online—The port is up and running. ■ Lock_Ref—The port is locking to the reference signal.
Comment field	The comment field follows the port state. The possible comments include: ■ Disabled—The port is disabled. ■ Loopback—The port is in loopback mode. ■ E_Port—The WWN and switch name of the other switch is shown, and the use of this ISL is shown. ■ F_Port—The WWN of the N_Port is shown. ■ G_Port—The port is online but is not yet an E_Port or F_Port. ■ L_Port—The port is connected to an arbitrated loop.

syslogdIp

Figure A-59 shows the syslogdIp command, which sets or displays the switch's system log daemon IP address. The command syntax is syslogdIp <"ip address">.

```
admin> syslogdIp

syslog daemon's address: 0.0.0.0
```

Figure A-59. syslogdIp command example

tempShow

Figure A-60 shows the tempShow command, which shows the switch's temperature as measured by five sensors on the motherboard.

```
admin> tempShow
 29  29  31  27  32 Centigrade
 84  84  87  80  89 Fahrenheit
```

Figure A-60. tempShow command example

uptime

Figure A-61 shows the uptime command, which displays the amount of time the switch has been in operation, the amount of time since the switch was first powered up, the date and time of the last reboot, and the reason for the last reboot.

For up and powered-on times less than 60 seconds, the time displays in seconds. For times greater than 60 seconds, the time displays in minutes.

```
switch:admin> uptime
Up for:3 days, 18:35
Powered for: 30 days, 16:05
Last up at: Mon Jan 11 16:17:29 1999
Reason:Reboot
```

Figure A-61. uptime command example

version

Figure A-62 shows the version command. The fields are described in the following table.

```
admin> version
Kernel: 5.3.1
Fabric OS: v2.0
Made on: Mon Nov 16 18:15:26 PST 1998
Flash: Mon Dec 28 15:34:05 PST 1998
BootProm: Thu Oct 1 13:34:29 PDT 1998
```

Figure A-62. version command example

Table A-18
version Command Field Descriptions

Field	Description
Kernel	Kernel operating environment version used on the processor
Fabric OS	Switch firmware version
Made on	Switch firmware release date and time
Flash	Build date of the firmware stored in flash memory
BootProm	Build date of the firmware stored in the boot prom

diagHelp

Figure A-63 shows the diagHelp command, which displays the diagnostic help commands available for troubleshooting switch problems.

```
switch:admin> diagHelp

ramTest                 System DRAM diagnostic
portRegTest             Port register diagnostic
centralMemoryTest       Central memory diagnostic
cmiTest                 CMI bus connection diagnostic
camTest                 Quickloop CAM diagnostic
portLoopbackTest        Port internal loopback diagnostic
sramRetentionTest       SRAM Data Retention diagnostic
cmemRetentionTest       Central Mem Data Retention diagnostic
crossPortTest           Cross-connected port diagnostic
spinSilk                Cross-connected line-speed exerciser
diagClearError          Clear diag error on specified port
diagDisablePost         Disable Power On Self-Test
diagEnablePost          Enable Power On Self-Test
setGbicMode             Enable tests only on ports with GBICs
setSplbMode             Enable 0=Dual, 1=Single
supportShow             Print the switch info for debugging
diagShow                Print diagnostic status information
parityCheck             Dram Parity 0=Disabled, 1=Enable
```

Figure A-63. diagHelp command example

licenseHelp

Figure A-64 shows the licenseHelp command, which displays the commands used to administer license keys. Each switch can save one license key for each optionally licensed product. License keys are unique for every switch.

```
switch:admin> licenseHelp

licenseAdd      Add a license key to this switch
licenseRemove   Remove a license key from this switch
licenseShow     Show current license key
```

Figure A-64. licenseHelp command example

qlHelp

Figure A-65 shows the qlHelp command, which displays the commands used to administer QuickLoop.

```
switch:admin> qlHelp

qlDisable       Disable quick loop mode
qlEnable        enable quick loop mode
qlPortDisable   Set portin non quick loop mode
qlPortEnable    Set port in quick loop mode
qlOnlineHold    Set hold loop in Monitoring option
qlOpenInitHold  Set hold loop in Open-Init option
qlPartner       Print/set quick loop partner
qlShow          Print quick loop info
```

Figure A-65. qlHelp command example

routeHelp

Figure A-66 shows the routeHelp command, which displays the routing help commands. Routing commands do not return relevant data unless the switch has a Fabric Operating System license.

```
admin> routeHelp

bcastShow          Print broadcast tree information
fspfShow           Print FSPF global information
interfaceShow      Print FSPF interface information
dlsReset           Turn off dynamic load sharing
dlsSet             Turn on the dynamic load sharing
iodReset           Turns off the in-order delivery option
iodSet             Turns on the in-order delivery option
LSDbShow           Print Link State Database entry
mcastShow          Print multicast tree information
nbrStateShow       Print neighbor's summary information
topologyShow       Print paths to domains
uRouteConfig       Configure static unicast route
uRouteRemove       Remove static unicast route
URouteShow         Print port's unicast routing info
```

Figure A-66. routeHelp command example

zoneHelp

Figure A-67 shows the zoneHelp command, which displays the zoning help commands.

```
switch:admin> zoneHelp

aliAdd             Add member to a zone alias
aliCreate          Create a zone alias
aliDelete          Delete a zone alias
aliRemove          Remove a member from a zone alias
aliShow            Print zone alias information
cfgAdd             Add a zone to a configuration
cfgCreate          Create a zone configuration
cfgDelete          Delete a zone configuration
cfgRemove          Remove a zone from a configuration
cfgShow            Print zone configuration information
zoneAdd            Add a member to a zone
zoneCreate         Create a zone
zoneDelete         Delete a zone
zoneRemove         Remove a member from a zone
zoneShow           Print zone information
cfgClear           Clear all zone configurations
cfgDisable         Disable a zone configuration
cfgEnable          Enable a zone configuration
cfgSave            Save zone configurations in flash
```

Figure A-67. zoneHelp command example

Diagnostic Commands

Diagnostic commands enable you to monitor, test, and evaluate the switch.

ramTest

Figure A-68 shows the ramTest command, which checks processor RAM memory. This test validates proper memory function.

```
switch:admin> ramTest

Running System DRAM Test ..... passed.
```

Figure A-68. ramTest command example

portRegTest

Figure A-69 shows the portRegTest command, which checks registers and static memory located on the motherboard. Registers are set under firmware control and are used to control the hardware route selection and other internal hardware functions. This test validates that all registers are accessible. This test cannot be executed on an operational switch. Before issuing the portRegTest command, disable the switch using the switchDisable command.

```
switch:admin> portRegTest

Running Port Register Test .... passed.
```

Figure A-69. portRegTest command example

centralMemoryTest

Figure A-70 shows the centralMemoryTest command, which checks the central memory in each Application Specific Integrated Circuit (ASIC). This test ensures that:

- The built-in self-repair (BISR) circuit in each ASIC chip does not report failure to repair bad cells (bisr test).
- The data cells can be uniquely written and read correctly (data write/read test).
- The data in any one ASIC can be read from any other ASIC (asic-asic test_).
- Bad parity can be detected and flagged in the error register and an interrupt can be posted (parity error test).

- Buffer number error can be detected and flagged in the error register and an interrupt can be posted (buffer number error test).
- Chip number error can be detected and flagged in the error register and an interrupt can be posted (chip number error test).

This test cannot be executed on an operational switch. Before issuing the centralMemoryTest command, disable the switch using the switchDisable command.

```
switch:admin> centralMemoryTest

Running Central Memory Test ... passed.
```

Figure A-70. centralMemoryTest command example

cmiTest

Figure A-71 shows the cmiTest command, which verifies that control messages can be correctly sent from any ASIC to any other ASIC. This command also tests the checksum check. This test cannot be executed on an operational switch. Before issuing the cmiTest command, disable the switch using the switchDisable command.

```
switch:admin> cmiTest

Running CMI Test ..... passed.
```

Figure A-71. cmiTest command example

camTest

Figure A-72 shows the camTest command, which verifies that the SID translation required by QuickLoop and implemented using content addressable memories (CAMs) is functioning correctly. This test cannot be executed on an operational switch. Before issuing the camTest command, disable the switch using the switchDisable command.

```
switch:admin> camTest

Running CAM Test ..... passed.
```

Figure A-72. camTest command example

portLoopbackTest

Figure A-73 shows the portLoopbackTest command, which verifies the intended functional operation of the switch by sending frames from each port's transmitter back to the same port's receiver through an internal hardware loopback. This command tests the switch circuitry up to the serial output of the ASIC. The command syntax is portLoopbackTest nFrames. This test cannot be executed on an operational switch. Before issuing the portLoopbackTest command, disable the switch using the switchDisable command.

If you do not include the nFrames parameter, the loopback test runs continuously until you press **Enter**.

```
switch:admin> portLoopbackTest
Running Port Loopback Test ....
Diags: (Q)uit, (C)ontinue, (S)tats, (L)og: s
Diagnostics Status: Sun Jan 1 00:00:00 2000

port#:    0     1     2     3     4     5     6     7
diags:    OK    OK    OK    OK    OK    OK    OK    OK
state:    UP    UP    UP    UP    UP    UP    UP    UP

      lm0:    4654  frTx     4654  frRx       0  LLI_errs.
      lm1:    4654  frTx     4654  frRx       0  LLI_errs.
      lm2:    4654  frTx     4654  frRx       0  LLI_errs.
      lm3:    4654  frTx     4654  frRx       0  LLI_errs.
      lm4:    4654  frTx     4654  frRx       0  LLI_errs.
      lm5:    4654  frTx     4654  frRx       0  LLI_errs.
      lm6:    4654  frTx     4654  frRx       0  LLI_errs.
      lm7:    4654  frTx     4654  frRx       0  LLI_errs.

Central Memory OK
Total Diag Frames Tx: 38032
Total Diag Frames Rx: 39232

Diags: (Q)uit, (C)ontinue, (S)tats, (L)og: q
  aborted
```

Figure A-73. portLoopbackTest command example

If the test does not find an error, there is no output. You can choose to continue the test, view statistics, or view an error log. The following table describes the loopback error message fields.

Table A-19
portLoopbackTest Command Field Descriptions

Field	Description
Diagnostics Status	The title header displays the time diagShow was executed.
port#	The port number.
diags	Port's current diagnostic status. Possible values include OK or BAD.
state	Port's current state. Possible values include UP (active) or DN (inactive).
lm0-7 (8-port) lm0-15 (16-port)	The frame counts of active ports. The display shows the number of frames transmitted and received and low level interface counts (LLI_errs).
Central Memory Status	Central memory status. Possible values include OK or FAULTY.
Total Diag Frames Tx	The total diagnostics frames transmitted (Tx) since boot. This number usually corresponds to the total frames received (Rx) but can differ because of failure modes.
Total Diag Frames Rx	The total diagnostics frames received (Rx) since boot. This number usually corresponds to the total frames transmitted (Tx) but can differ because of failure modes.

sramRetentionTest

Figure A-74 shows the sramRetentionTest command, which verifies that data written into the ASIC memories are retained and that data bits do not decrease when read after some amount of delay since the write. This test cannot be executed on an operational switch. Before issuing the sramRetentionTest command, disable the switch using the switchDisable command.

```
switch:admin> sramRetentionTest

Running SRAM Retention Test ..... passed.
```

Figure A-74. sramRetentionTest command example

cmemRetentionTest

Figure A-75 shows the cmemRetentionTest command, which verifies that data written into the SRAMs that make up the central memory is retained and that data bits do not decrease when read after some amount of delay since the write. This test cannot be executed on an operational switch. Before issuing the cmemRetentionTest command, disable the switch using the switchDisable command.

```
switch:admin> cmemRetentionTest

Running cmemRetention Test ..... passed.
```

Figure A-75. cmemRetentionTest command example

crossPortTest

Figure A-76 shows the crossPortTest command, which verifies the intended functional operation of the switch. Each port's transmitter sends frames by means of the GBIC module and external cable to another port's receiver. This test exercises the entire path of the switch.

You can connect any port to any other port in the same switch provided the connection is of the same technology, for example, GBIC-SW ports to GBIC-SW ports and GBIC-LW ports to GBIC-LW ports.

NOTE: All ports on the switch must be connected if the GBIC mode is disabled or if the switch shows an error condition. When running the Cross Port test, set the operating mode value to 0 or 1.

```
switch:admin> crossPortTest

Running Cross Port Test .....
switchName: JR-6011
switchType: 3.1
switchState: Testing
switchRole: Disabled
switchDomain: 1 (unconfirmed)
switchId: fffc01
switchWwn: 10:00:00:60:69:00:60:11
port 0: sw Testing Loopback->1
port 1: sw Testing Loopback->0
port 2: sw Testing Loopback->7
port 3: sw Testing Loopback->6
port 4: sw Testing Loopback->5
port 5: sw Testing Loopback->4
port 6: sw Testing Loopback->3
port 7: sw Testing Loopback->2

Port SNMP    Physical        Flags
--------------------------------
  0: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  1: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  2: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  3: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  4: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  5: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  6: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  7: Testing  In_Sync      PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED CBL_LB LOGIN
  8: Testing  UNKNOWN      PRESENT ACTIVE G_PORT
```

Figure A-76. crossPortTest command example

Cross Port Test Modes

The Cross Port test behaves differently according to the activated modes.

switchEnabled or switchDisabled mode

- Online mode (switch enabled before executing the test)—In the Online mode, only ports cable loopbacked to ports in the same switch are tested. The test ignores ports connected outside of the switch. To be successful, the test must find at least one port (if the singlePortAlso mode is active) or two ports (if the singlePortAlso mode is not active) cable loopbacked to each other. If not, the test displays the following message:

  ```
  Need at least 1 port(s) connected to run this test.

  OR

  Need at least 2 port(s) cross-connected to run this test.
  ```

- Offline mode (switch disabled before executing the test)—In the Offline mode, all ports cable loopbacked to similar ports in the same switch are tested. The test aborts if one or more ports are not connected. If any pair of ports is improperly connected (improperly seated GBIC modules or cables, bad GBIC modules or cables, improper connection of SW to LW, and so on), the following message displays:

  ```
  One or more ports is not active, please double-check fibres on all ports.
  ```

singlePortAlso mode

Specify the singlePortAlso mode by executing the Cross Port test with a second argument value of one.

```
sw:admin> crossPortTest 0, 1
```

In this mode, the Cross Port test allows a port to be cable loopbacked to itself (port M is connected to port M) in addition to the supported cross connection (port M is connected to port N). This configuration can be used to isolate bad ports.

GBIC mode

Activate the GBIC mode by executing the following command before executing the Cross Port test:

```
sw:admin> setGbicMode 1
```

When activated, only ports with GBIC modules present are tested. The state of the GBIC mode is activated until it is disabled as follows:

```
sw:admin> setGbicMode 0
```

An example mode of operation would be to disable the switch, set the GBIC mode to 1, and execute the Cross Port test with the singlePortAlso mode activated to limit testing to:

- Ports with GBIC modules installed
- Ports properly cable loopbacked
- Ports connected to themselves (single port connections)

The command syntax is:

```
crossPortTest <nFrames>, <0 or 1>
```

where <nFrames> determines the number of frames to run, and <0 or 1> determines if a single port connection is allowed (0=not allowed, 1=allowed). If you do not include the <nFrames> parameter, the test runs until you press **Enter**.

spinSilk

Figure A-77 to Figure A-79 show the spinSilk command, which verifies the intended functional operation of the switch. Each port's transmitter sends frames by means of the GBIC module and external cable to another port's receiver at full hardware speed (1 GB/s). The entire path of the switch is exercised. Because the processor does not compare data on each frame, the Spin Silk test does not report the DIAG-DATA error. Other error messages defined for the Cross Port test and the corresponding probable causes and actions are applicable to the Spin Silk test.

The state of the GBIC mode affects the operation of the Spin Silk test. To activate the GBIC mode, execute the following command prior to executing the crossPortTest command:

```
switch:admin> setGbicMode 1
```

When activated, only ports with GBIC modules installed are included in the Spin Silk test's list of ports to test. For example, if only ports 0 and 3 have GBIC modules installed and the GBIC mode is activated, the Spin Silk test limits testing to ports 0 and 3. The state of the GBIC mode is saved in flash memory. The GBIC mode stays activated (even after reboots or power cycles) until you disable it with the following command:

```
sw:admin> setGbicMode 0
```

An example mode of operation would be to disable the switch, set the GBIC mode to 1, and execute the Spin Silk test to limit testing to:

- Ports with GBIC modules installed
- Ports that are properly cable loopbacked

IMPORTANT: This test cannot be executed on an operational switch. Before issuing the spinSilk command, disable the switch using the switchDisable command.

NOTE: When running the Spin Silk test, you must set the operating mode value to 0 or 1. Using operating mode 0 when running the Spin Silk test is recommended.

The command syntax is:

```
spinSilk nMillions
```

where nMillions is the number of frames for the test to execute expressed in millions of frames. If you do not include the nMillions parameter, the Spin Silk test runs until you press **Enter**.

```
switch:admin> spinSilk 2
Running Spin Silk .....
One moment please ...
switchName: SR-7371
switchType: 2.2
switchState: Testing
switchRole: Disabled
switchDomain: 1 (unconfirmed)
switchId: fffc01
switchWwn: 10:00:00:60:69:00:73:71
port 0: cu Testing Loopback->15
port 1: sw Testing Loopback->11
port 2: sw Testing Loopback->7
port 3: lw Testing Loopback->4
port 4: lw Testing Loopback->3
port 5: sw Testing Loopback->9
port 6: sw Testing Loopback->14
port 7: sw Testing Loopback->2
port 8: sw Testing Loopback->13
port 9: sw Testing Loopback->5
port 10: sw Testing Loopback->12
port 11: sw Testing Loopback->1
port 12: sw Testing Loopback->10
port 13: sw Testing Loopback->8
port 14: sw Testing Loopback->6
port 15: cu Testing Loopback->0
Transmitting ... done.
Spinning ...
port 15 Rx/Tx 1 of 2 million frames.
port 0 Rx/Tx 1 of 2 million frames.
port 1 Rx/Tx 1 of 2 million frames.
port 2 Rx/Tx 1 of 2 million frames.
port 3 Rx/Tx 1 of 2 million frames.
port 4 Rx/Tx 1 of 2 million frames.
port 5 Rx/Tx 1 of 2 million frames.
port 6 Rx/Tx 1 of 2 million frames.
port 7 Rx/Tx 1 of 2 million frames.
```

Figure A-77. spinSilk command example 1

```
port 8 Rx/Tx 1 of 2 million frames.
port 9 Rx/Tx 1 of 2 million frames.
port 10 Rx/Tx 1 of 2 million frames.
port 11 Rx/Tx 1 of 2 million frames.
port 12 Rx/Tx 1 of 2 million frames.
port 13 Rx/Tx 1 of 2 million frames.
port 14 Rx/Tx 1 of 2 million frames.
port 8 Rx/Tx 2 of 2 million frames.
port 9 Rx/Tx 2 of 2 million frames.
port 10 Rx/Tx 2 of 2 million frames.
port 11 Rx/Tx 2 of 2 million frames.
port 12 Rx/Tx 2 of 2 million frames.
port 13 Rx/Tx 2 of 2 million frames.
port 14 Rx/Tx 2 of 2 million frames.
port 15 Rx/Tx 2 of 2 million frames.
port 0 Rx/Tx 2 of 2 million frames.
port 1 Rx/Tx 2 of 2 million frames.
port 2 Rx/Tx 2 of 2 million frames.
port 3 Rx/Tx 2 of 2 million frames.
port 4 Rx/Tx 2 of 2 million frames.
port 5 Rx/Tx 2 of 2 million frames.
port 6 Rx/Tx 2 of 2 million frames.
port 7 Rx/Tx 2 of 2 million frames.
```

Figure A-78. spinSilk command example 1 (continued)

```
Diagnostics Status: Thu Jul 30 14:43:36 1998

port#:  0   1   2   3   4   5   6   7   8   9 10  11  12  13  14  15
diags: OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK  OK
state: UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP  UP
   lm0:  2044334  frTx    2053602  frRx     0  LLI_errs. <looped-15>
   lm1:  2046987  frTx    2049307  frRx     0  LLI_errs. <looped-11>
   lm2:  2046259  frTx    2050415  frRx     0  LLI_errs. <looped-7>
   lm3:  2048907  frTx    2038532  frRx     0  LLI_errs. <looped-4>
   lm4:  2038717  frTx    2049093  frRx     0  LLI_errs. <looped-3>
   lm5:  2049555  frTx    2052277  frRx     0  LLI_errs. <looped-9>
   lm6:  2048260  frTx    2047600  frRx     0  LLI_errs. <looped-14>
   lm7:  2051407  frTx    2047246  frRx     0  LLI_errs. <looped-2>
   lm8:  2055484  frTx    2048350  frRx     0  LLI_errs. <looped-13>
   lm9:  2053018  frTx    2050297  frRx     0  LLI_errs. <looped-5>
   lm10: 2048345  frTx    2048404  frRx     0  LLI_errs. <looped-12>
   lm11: 2051282  frTx    2048962  frRx     0  LLI_errs. <looped-1>
   lm12: 2048944  frTx    2048885  frRx     0  LLI_errs. <looped-10>
   lm13: 2049535  frTx    2056672  frRx     0  LLI_errs. <looped-8>
   lm14: 2049481  frTx    2050141  frRx     0  LLI_errs. <looped-6>
   lm15: 2056950  frTx    2047666  frRx     0  LLI_errs. <looped-0>

Central Memory OK
Total Diag Frames Tx: 130432
Total Diag Frames Rx: 134752
```

Figure A-79. spinSilk command example 2

diagClearError

Figure A-80 shows the diagClearError command, which clears diagnostic errors detected on a specified port. Issuing this command does not clear the error log. The command syntax is diagClearError <port #>. Without the <port #> parameter, all errors are cleared.

```
switch:admin> diagClearError
```

Figure A-80. diagClearError command example

diagDisablePost

Figure A-81 shows the diagDisablePost command, which disables POST processing. The boot time without POST processing is approximately 50 to 55 seconds. A switch rebooted without POST generates the DIAG-POST_SKIPPED error.

NOTE: Always execute POST processing to ensure the operational status of the switch during the power up stage.

```
switch:admin> diagDisablePost

Committing configuration...done.

On next reboot, POST will be skipped.
```

Figure A-81. diagDisablePost command example

diagEnablePost

Figure A-82 shows the diagEnablePost command, which enables POST processing. The boot time with POST processing is approximately 110 to 120 seconds for warm POST, and 165 to 175 seconds for cold POST. POST processing is enabled by default.

```
switch:admin> diagEnablePost

Committing configuration...done.

On next reboot, POST will be executed.
```

Figure A-82. diagEnablePost command example

setGbicMode

The GBIC mode, when enabled, forces the Cross Port test or the Spin Silk test to limit testing to only ports with detected GBIC modules. To enable GBIC mode, execute the setGbicMode 1 command.

```
switch:admin> setGbicMode 1
```

Figure A-83. setGbicMode 1 command example

To disable GBIC mode, execute the setGbicMode 0 command.

```
switch:admin> setGbicMode 0
```

Figure A-84. setGbicMode 0 command example

setSplbMode

Figure A-85 shows the setSplbMode command, which enables and disables the SPLB mode. The parameter can be set to "0" or "1". When set to "0', the SPLB mode is disabled. When set to "1', the SPLB mode is enabled. The default setting is "0".

The mode is saved in flash memory and stays in that mode until the next execution of setSplbMode. Rebooting is not required to execute the command.

When enabled, the SPLB mode forces spinSilk to disable two port loop-back for M-> M connected ports. This may be useful to isolate internal switch problems from GBIC problems since the internal paths are used much less with SPLB mode enabled.

When disabled, the SPLB mode forces spinSilk to circulate frames between pairs of M->M connected ports as follows:

P1 TX >>> P1 RX -> P2 TX >>> P2 RX -> P1 TX
>>> cable or internal loop-back
-> routing table entry

The connections between pairs of M->M ports exercise the connections between as many chips (or bloom quadrants) as possible subject to the setting of allow_intra_chip and the availability of pairs M->M ports.

Any ports that are cross-cabled are routed to each other in the normal manner regardless of the setting of the SPLB mode:

P1 TX >>> P2 RX -> P1 TX and
P2 TX >>> P1 RX -> P2 TX

```
switch:admin> setSplbMode 1
Committing configuration…done.
SPLB mode is now ON.

switch:admin> setSplbMode 0
Committing configuration…done.
SPLB mode is now OFF.
```

Figure A-85. setSplbMode command example

supportShow

The supportShow command prints switch information for debugging purposes. The command executes the following commands in the order shown:

- version
- tempShow
- psShow
- licenseShow
- diagShow
- errDump
- switchShow
- portFlagsShow
- portErrShow
- mqShow
- portSemShow
- portShow
- portRegShow
- portRouteShow
- fabricShow
- topologyShow
- qlShow
- nsShow
- nsAllShow
- cfgShow
- configShow
- faultShow
- traceShow
- portLogDump

Figure A-86 shows the supportShow command. The command syntax is:

supportShow <firstPort>, <lastPort>, <nLog>

```
switch:admin> supportShow
VxWorks: 5.3.1
Firmware: v2.0_beta3
Made on: Fri Mar 19 16:29:55 PST 1999
Flash: Fri Mar 19 16:30:19 PST 1999
BootProm: Tue Dec 29 17:32:38 PST 1998
none:
No licenses
28 29 30 29 27 Centigrade
82 84 86 84 80 Fahrenheit
Power Supply #1 is absent
Power Supply #2 is OK
```

Figure A-86. supportShow command example

Table A-20 describes the supportShow command fields.

Table A-20
supportShow Field Descriptions

Field	Description
firstPort	The first port in a range of ports about which information is printed. The default (if no operand is specified) is to print the state of port 0. If only firstPort is specified, only the information for firstPort is printed.
lastPort	The last port in a range of ports about which information is printed. If firstPort is specified but lastPort is not specified, only firstPort information is printed for the port-based commands (portShow, portRegShow, and portRouteShow).
nLog	Number of lines of portLogDump to print: ■ 0 means dump all lines (default) ■ N means dump the last N lines ■ <0 means skip portLogDump

diagShow

Figure A-87 shows the diagShow command, which summarizes the diagnostics results, including POST results, since the switch was last booted. Table A-21 describes the fields.

The diagShow command can be looped. For example, diagShow 4 executes diagShow every four seconds until you stop it by pressing **Enter**. This command can be used to isolate a bad GBIC module. A port with a changing LLI_errs value is prefixed by ** in the display.

```
switch:admin> diagShow

Diagnostics Status: Sun Jan 1 00:00:00 2000

port#:  0   1   2   3   4   5   6   7   8   9 10 11 12 13 14 15
diags: OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK OK
state: UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP UP

  lm0:  39624101  frTx     40128685  frRx     0  LLI_errs. <looped-15>
  lm1:  39309877  frTx     40007305  frRx     0  LLI_errs  <looped-11>
  lm2:  39750791  frTx     39885106  frRx     0  LLI_errs. <looped-6>
  lm3:  39501243  frTx     40065867  frRx     0  LLI_errs. <looped-4>
  lm4:  40066092  frTx     39501463  frRx     0  LLI_errs. <looped-3>
  lm5:  40075160  frTx     40257190  frRx     0  LLI_errs. <looped-8>
  lm6:  39886034  frTx     39751716  frRx     0  LLI_errs. <looped-2>
  lm7:  39989371  frTx     39960595  frRx     0  LLI_errs. <looped-12>
  lm8:  40257892  frTx     40075855  frRx     0  LLI_errs. <looped-5>
  lm9:  39154671  frTx     40250787  frRx     0  LLI_errs. <looped-14>
  lm10: 39767848  frTx     39798346  frRx     0  LLI_errs. <looped-13>
  lm11: 40009605  frTx     39312144  frRx     0  LLI_errs. <looped-1>
  lm12: 39961890  frTx     39990666  frRx     0  LLI_errs. <looped-7>
  lm13: 39799377  frTx     39768879  frRx     0  LLI_errs. <looped-10>
  lm14: 40252478  frTx     39156315  frRx     0  LLI_errs. <looped-9>
  lm15: 40132745  frTx     39628100  frRx     0  LLI_errs. <looped-0>

Central Memory OK
Total Diag Frames Tx: 419264
Total Diag Frames Rx: 447200
```

Figure A-87. diagShow command example

Table A-21
diagShow Command Field Descriptions

Field	Description
Diagnostics Status	The title header displays the time diagShow was executed.
port#	The port number.
diags	Port's current diagnostic status. Possible values include OK or BAD.
state	Port's current state. Possible values include UP (active) or DN (inactive).
lm0-7 (8-port) lm0-15 (16-port)	The frame counts of active ports. The display shows the number of frames transmitted and received and low level interface counts (LLI_errs).
Central Memory Status	Central memory status. Possible values include OK or FAULTY.
Total Diag Frames Tx	The total diagnostics frames transmitted (Tx) since boot. This number usually corresponds to the total frames received (Rx) but can differ because of failure modes.
Total Diag Frames Rx	The total diagnostics frames received (Rx) since boot. This number usually corresponds to the total frames transmitted (Tx) but can differ because of failure modes.

parityCheck

Figure A-88 shows the parityCheck command, which enables and disables the DRAM parity checking. The parameter can be set to "0" or "1". When set to "0', the DRAM parity checking mode is disabled. When set to "1', the DRAM parity checking mode is enabled. The default setting is "0".

The mode is saved in flash memory and stays in that mode until the next execution of parityCheck. Rebooting is not required to execute the command.

When enabled, the DRAM parity checking causes ramTest to perform several additional tests of the parity memory. It also enables the parity checking hardware to verify proper parity on all DRAM read operations.

```
switch:admin> parityCheck 1
Committing configuration…done.
Parity check is now ON.

switch:admin> parityCheck 0
Committing configuration…done.
Parity check is now OFF.

switch:admin> parityCheck 0
Parity not supported on system model: 4
Parity check already OFF.
```

Figure A-88. parityCheck command example

Routing Commands

Routing commands let you view switch routing information. Routing commands only return relevant data for switches that have the Fabric Operating System license installed.

bcastShow

Figure A-89 shows the bcastShow command, which displays broadcast tree information and all ports that are currently transmitting and receiving broadcast frames. The fields are described in the following table.

The bcastShow command helps you understand the routes the broadcast frames take through the fabric. A bit set indicates that the corresponding port belongs to a specific set. For instance, the bitmap value 0x00010003 means that port 0, port 1, and port 16 (the embedded port) are members of the set.

```
admin> bcastShow

Group   Member Ports       Member ISL Ports   Static ISL Ports
--------------------------------------------------------------
31      0x00010003         0x00000000         0x00000000
```

Figure A-89. bcastShow command example

Table A-22
bcastShow Bitmap Field Descriptions

Bitmap Field	Description
Group	The multicast group
Member Ports	All ports currently transmitting or receiving broadcast frames
Member ISL Ports	Ports that belong to the interswitch broadcast distribution tree, as selected by the dynamic broadcast path selection protocol. Broadcast frames use these ports to reach all of the fabric switches and to enter into the switch. Some of the E_Ports on a switch cannot be part of this set since the broadcast paths must constitute a tree.
Static ISL Ports	Ports that belong to the interswitch broadcast distribution tree, as configured through the shell. This field is normally 0x00000000.

fspfShow

Figure A-90 shows the fspfShow command, which displays Fibre Channel Shortest Path First (FSPF) information. The fields are described in the following table.

```
switch:admin> fspfShow

version          = 2
domainID         = 1
isl_ports        = 0x00000000
minLSArrival     = 3
minLSInterval    = 5
LsoriginCount    = 0
startTime        = 18656
fspfQ            = 0x10fa44e0
fabP             = 0x10fa4d60
agingTID         = 0x10f7e4c0
agingTo          = 10000
lsrDlyTID        = 0x10f6e4f0
lsrDelayTo       = 5000
lsrDelayCount    = 0
ddb_sem          = 0x10fa44b0

fabP:
event_sch = 0x0
lsrRefreshCnt = 0
```

Figure A-90. fspfShow command example

Table A-23
fspfShow Command Field Descriptions

Field	Description
version	The version of the FSPF protocol
domainID	The local switch's domain ID
isl_ports	A bitmap field that shows all local switch E_Ports
startTime	The time the FSPF started, in milliseconds from boot.
other	Internal FSPF variables

interfaceShow

Figure A-91 shows the interfaceShow command, which displays FSPF interface information. This includes static information about the port (for example, variables allocated when a port is down) and "neighbor" information (variables associated with the remote switch connected to the port). An FSPF interface corresponds to an E_Port. The fields are described in Table A-24.

The command syntax is interfaceShow <port#>. With no parameters, the command result shows the information for all switch interfaces.

```
switch:admin> interfaceShow
idbP              = 0x10f7e560
Interface 10 data structure:
nghbP             = 0x0
ifNo              = 0
cost              = 1000
delay             = 1
lastScn           = 5
lastScnTime       = Mar 20 16:09:49.199
upCount           = 0
lastUpTime        = Mar 20 16:09:49.199
downCount         = 2
lastDownTime      = Mar 20 16:09:46.516
downReason        = 2
iState            = DOWN

Type <CR> to continue, Q<CR> to stop:
```

Figure A-91. interfaceShow command example

```
Neighbor 10 data structure:
state           = NB_ST_FULL
nghbCap         = 0x0
nghbId          = 239
idbNo           = 10
remPort         = 10
nflags          = 0x3
initCount       = 1
&dbRetransList  = 0x10e83530
&lsrRetransList = 0x10e83540
&lsrAckList     = 0x10e83550
inactTID        = 0x10e83200
helloTID        = 0x10e834c0
dbRtxTID        = 0x10e833d0
lsrRtxTID       = 0x10e82cb0
inactTo         = 80000
helloTo         = 20000
rXmitTo         = 5000
nCmdAcc         = 132
nInvCmd         = 0
nHloIn          = 122
nInvHlo         = 0
nLsuIn          = 5
nLsaIn          = 5
attHloOut       = 123
nHloOut         = 123
attLsuOut       = 5
nLsuOut         = 5
attLsaOut       = 5
nLsaOut         = 5
```

Figure A-92. interfaceShow command example (continued)

Table A-24
interfaceShow Command Field Descriptions

Field	Description
idbP	The port number
nghbP	The neighbor (adjacent) switch's port
ifNo	The port number, which should be identical to the value specified in the command line

continued

Table A-24
interfaceShow Command Field Descriptions *continued*

Field	Description
cost	The cost of sending a frame over the ISL connected to this port. The value 1000 indicates a 1 Gbps link.
delay	The conventional delay incurred by a frame transmitted on this ISL. The delay is required by the FSPF protocol and is a fixed value.
lastScn	The last State Change Notification received on this interface.
lastScnTime	The time the last SCN was received.
upCount	The number of times this interface initialized (the transition number from an offline to E_Port state)
lastUpTime	The last time this interface came up.
downCount	The number of times this interface went down.
lastDownTime	The last time this interface went down.
downReason	The reason (SCN) for the interface going down.
iState	The current interface state, which must be up in order for the ISL to forward frames to the adjacent switch
state	The current neighbor state. The state value must be NB_ST_FULL for the ISL to forward frames to the adjacent switch. Other values can be transitory; however, if a value is retained for more than 10 seconds, contact technical support.
nghbCap	Neighbor capabilities have a value of 0.
nghbId	The neighbor (adjacent) switch's domain ID
idbNo	The port number
remPort	The port number on the remote switch connected to this port
inactTo	The inactivity time out (in milliseconds). When this timeout expires, the adjacency with the neighbor switch expires. When this happens, new paths are computed to all possible destination switches in the fabric.
helloTo	The Hello timeout. When this timeout expires, a Hello frame is sent to the neighbor switch through this port.
rXmitTo	The retransmit timeout, which is used to transmit topology information to the neighbor switch. If an acknowledgment is not received within rXmitTo, the frame is retransmitted.

continued

Table A-24
interfaceShow Command Field Descriptions *continued*

Field	Description
nCmdAcc	The number of commands accepted from the neighbor switch, which include Hellos, Link State Updates, and Link State Acknowledges
nInvCmd	The number of invalid commands received from the neighbor switch. These are commands with a version higher than the one running on the local switch. The current version is 1 and there is no version 0.
nHloIn	The number of Hello frames received from the neighbor switch
nInvHlo	The number of invalid Hello frames received from the neighbor switch. These are Hello frames with invalid parameters.
nLsuIn	The number of Link State Updates received from the neighbor switch
nLsaIn	The number of Link State Acknowledges received from the neighbor switch
attHloOut	The number of attempted transmissions of Hello frames to the neighbor switch
nHloOut	The number of Hello frames actually transmitted to the neighbor switch
attLsuOut	The number of attempted transmissions of Link State Updates to the neighbor switch
nLsuOut	The number of Link State Updates actually transmitted to the neighbor switch
attLsaOut	The number of attempted transmissions of Link State Acknowledgments to the neighbor switch
nLsaOut	The number of Link State Acknowledgments actually transmitted to the neighbor switch
other	The other fields represent internal FSPF variables.

dlsReset

Figure A-93 shows the dlsReset command, which turns off the dynamic load sharing option. The dlsReset command prevents load sharing when a fabric change occurs if otherwise working ports could be affected. Load sharing will only occur when a switch reboots. Only use this command if devices connected to the fabric cannot properly handle occasional routing changes. Optimal load sharing is rarely achieved with this setting.

```
switch:admin> dlsReset
```

Figure A-93. dlsReset command example

dlsSet

Figure A-94 shows the dlsSet command, which allows load sharing when a fabric change occurs. Routing is done on a per source port basis. All traffic coming in from a port that is directed to the same remote domain is routed through the same output E_Port. To optimize fabric utilization, traffic is shared among all paths when there are multiple equivalent paths to a remote switch. If dynamic load sharing is enabled, the optimal load sharing is recomputed every time a change in the fabric occurs. By default, the load sharing option is on.

When dynamic load sharing is set, routing changes can affect working ports and applications, especially if the in-order delivery option is set.

```
switch:admin> dlsSet
```

Figure A-94. dlsSet command example

iodReset

Figure A-95 shows the iodReset command, which turns off the in-order delivery option. This command allows out-of-order delivery of frames during fabric topology changes. After you execute the iodReset command, the switch allows fast rerouting after a fabric topology change. Use the configShow command to view the status of the iodReset command. If the route.delay.Reroute parameter is equal to 0, the in-order delivery option is off.

```
switch:admin> iodReset
```

Figure A-95. iodReset command example

iodSet

Figure A-96 shows the iodSet command, which ensures that frames will not be delivered out-of-order, even during fabric topology changes. In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. Use the configShow command to view the status of the iodSet command. If the route.delay.Reroute parameter is equal to 1, the in-order delivery option is on.

Use this command with care because it will cause a delay in the establishment of a new path when a topology change occurs. Only use this command if there are devices connected to the fabric that do not tolerate occasional out-of-order delivery of frames. By default, the in-order delivery option is on.

```
switch:admin> iodSet
```

Figure A-96. iodSet command example

LSDbShow

Figure A-97 shows the LSDbShow command, which displays domain Link State Database entries. The fields are described in Table A-25. The database record for any fabric switch can be displayed from any switch. The LSDbShow command gives the same information regardless of which switch is used to run the program (unless there is a database update in progress, which occurs every 10 minutes in a stable network).

Every switch keeps a database of topology information associated with itself and the other fabric switches. The topology information for a switch consists of all neighbors that are in NB_ST_FULL state and the associated port numbers.

This replicated database remains in sync at all times so that every switch in the fabric has the same topology view. The topology database, in turn, is used to compute the path from a switch to all other fabric switches.

With no parameters specified, the command shows all of the Link State Records (LSR) in the database instead of the LSR for domain 1.

```
admin> LSDbShow
Domain=0, Link State Database Entry pointer=0x10393140
lsrP                = 0x1036b650
earlyAccLSRs        = 0
ignoredLSRs         = 0
lastIgnored         = Never
installTime         = 0x96a64 (617060)
lseFlags            = 0xa
uOutIfs             = 0x2000
uPathCost           = 1000
uHopsFromRoot       = 1
mOutIfs             = 0x0
parent              = 0x0
mPathCost           = 0
mHopsFromRoot       = 0

Link State Record:
Link State Record pointer = 0x1036b650
lsAge               = 512
reserved            = 0
type                = 1
options             = 0x0
lsId                = 0
advertiser          = 0
incarn              = 0x800003a0
length              = 60
chksum              = 0x9afe
linkCnt = 2,        flags = 0x0
LinkId = 1, out port = 8, rem port = 13, cost = 1000, costCnt = 0, type = 1
LinkId = 2, out port = 9, rem port =  8, cost = 1000, costCnt = 0, type = 1
```

Figure A-97. LSDbShow command example

Table A-25
LSDbShow Command Field Descriptions

Field	Description
domain	Indicates that domain 1 is the local switch's domain ID
lsrP	Link State Database Entry pointer
earlyAccLSRs	The number of LSRs (Link State Records) accepted within the 5-second window
ignoredLSRs	The number of LSRs ignored because the time was inside the 5-second window
lastIgnored	The time the last LSR was ignored because it was inside the 5-second window
installTime	This is the database entry for domain 1. The keyword installTime is the time when this database record was installed, in milliseconds from boot. Values are in hexadecimal and decimal format.
debug fields	These fields contain internal Fibre Channel Shortest Path First (FSPF) information and are used by customer support for debugging purposes only: lseFlags, uOutIfs, uPathCost, uHopsFromRoot, mOutIfs, parent, mPathCost, and mHopsFromRoot.
lsAge	The record age in seconds since installation time. Records are refreshed throughout the fabric every 30 minutes. This value should never exceed 3600. When lsAge reaches the value 1800, the record is flushed from the fabric if the switch that is described by the LSR is functioning and is connected to the fabric.
reserved	This field is reserved for internal use.
type	Always 1
options	Default 0
lsId	The record's Link State ID is equal to the switch's domain ID, as described by the record.
advertiser	The switch ID of the switch that issued this LSR. Default set to lsId.
incarn	The incarnation number. When a record is refreshed every 10 minutes, its incarnation number is incremented by 1. If data in the record changes (for example, if an E_Port on a switch goes offline), the switch described by that record issues a new instance and increments the incarnation number by 1.
length	The total record length

continued

Table A-25
LSDbShow Command Field Descriptions *continued*

Field	Description
chksum	The record checksum, which includes all fields except lsAge.
linkCnt	The link count, which is the number of neighbors in NB_ST_FULL state that are adjacent to the switch described by this record. The linkCnt field is followed by a number of lines equal to the link count. Each line contains the following information: ■ linkID—The neighbor switch's domain ID. ■ out port—The ISL port number connecting the neighbor switch. ■ cost—The cost of sending a frame over the ISL connected to this port. The cost is the same value as the cost in the neighbor data structure of the switch described by this record.
linkID	The neighbor switch's domain ID
rem port	The port on the remote switch that the local port (out port) is connected to
costCnt	Always 0
type	Always 1

mcastShow

Figure A-98 and Figure A-99 show the mcastShow command with and without a parameter (group number). Without parameters, this command shows multicast tree information for all of the multicast groups. With parameters, it shows information about one multicast group only. Table A-26 describes the command fields.

```
admin> mcastShow
Group   Member Ports    Member ISL Ports   Static ISL Ports
-------------------------------------------------------------------
  0     0x00000084     0x00000084         0x00000000
  1     0x00000084     0x00000084         0x00000000
  2     0x00000084     0x00000084         0x00000000
  3     0x00000084     0x00000084         0x00000000
  4     0x00000084     0x00000084         0x00000000
  5     0x00000084     0x00000084         0x00000000
  6     0x00000084     0x00000084         0x00000000
  7     0x00000084     0x00000084         0x00000000
  8     0x00000084     0x00000084         0x00000000
  9     0x00000084     0x00000084         0x00000000
 10     0x00000084     0x00000084         0x00000000
 11     0x00000084     0x00000084         0x00000000
 12     0x00000084     0x00000084         0x00000000
 13     0x00000084     0x00000084         0x00000000
 14     0x00000084     0x00000084         0x00000000
 15     0x00000084     0x00000084         0x00000000
 16     0x00000084     0x00000084         0x00000000
 17     0x00000084     0x00000084         0x00000000
 18     0x00000084     0x00000084         0x00000000
 19     0x00000084     0x00000084         0x00000000
 20     0x00000084     0x00000084         0x00000000
 21     0x00000084     0x00000084         0x00000000
 22     0x00000084     0x00000084         0x00000000
 23     0x00000084     0x00000084         0x00000000
 24     0x00000084     0x00000084         0x00000000
 25     0x00000084     0x00000084         0x00000000
 26     0x00000084     0x00000084         0x00000000
 27     0x00000084     0x00000084         0x00000000
 28     0x00000084     0x00000084         0x00000000
 29     0x00000084     0x00000084         0x00000000
 30     0x00000084     0x00000084         0x00000000
 31     0x00010087     0x00000084         0x00000000
```

Figure A-98. mcastShow command example 1

```
admin> mcastShow 1
Group   Member Ports    Member ISL Ports   Static ISL Ports
-------------------------------------------------------------------
  1     0x00000011     0x00000011         0x00000000
```

Figure A-99. mcastShow command example 2

Table A-26
mcastShow Bitmap Field Descriptions

Bitmap Field	Description
Group	The multicast group
Member Ports	All ports currently transmitting or receiving broadcast frames
Member ISL Ports	Ports that belong to the interswitch broadcast distribution tree, as selected by the dynamic broadcast path selection protocol. These are all E_Ports, and this set is a subset of m_port. Broadcast frames use these ports to reach all fabric switches and to enter into the switch. Some of the E_Ports on a switch may not be part of this set since the broadcast paths must constitute a tree.
Static ISL Ports	Ports that belong to the interswitch broadcast distribution tree, as configured through the shell. This field is normally 0x00000000.

nbrStateShow

Figure A-100 and Figure A-101 show the nbrStateShow command, which displays the neighbor's summary information. You can also see this information by using the interfaceShow command. The nbrStateShow command provides essential information to determine the fabric topology in a concise way. By using this command, you can discover the domain ID of all switches directly connected to the local switch and the port number on the local and remote switches. The command fields are described in Table A-27.

With no parameters, the nbrStateShow command shows the neighbor's state summary for all of the neighbors instead of the neighbor connected to port 0 only. The command syntax to list all neighbors is nbrStateShow.

```
admin> nbrStateShow

Local Domain ID: 1

Local Port      Domain      Remote Port          State
-------------------------------------------------------------------
    0             2             0             NB_ST_FULL
    1             2             1             NB_ST_FULL
    2             2             2             NB_ST_FULL
    4             5             4             NB_ST_FULL
    5             5             5             NB_ST_FULL
    7             5             6             NB_ST_FULL
```

Figure A-100. nbrStateShow command example 1

The command syntax is nbrStateShow <port #> to list the neighbor on the specified port.

```
admin> nbrStateShow 1

Local Domain ID: 3

Local Port      Domain      Remote Port          State
-------------------------------------------------------------------
  1               2             1              NB_ST_FULL
```

Figure A-101. nbrStateShow command example 2

Table A-27
nbrStateShow Command Field Descriptions

Field	Description
Local Port	Corresponds to idbNo in the neighbor data structure.
Domain	Corresponds to nghbId in the neighbor data structure.
Remote Port	Corresponds to remPort in the neighbor data structure.
State	The neighbor's current state. The state value must be NB_ST_FULL for the ISL to forward frames to the adjacent switch. Other values can be transitory; however, if a value is retained for more than 10 seconds, contact technical support.

topologyShow

Figure A-102 and Figure A-103 show the topologyShow command, which displays all paths to a domain including:

- Output ports used to route frames to the domain
- The routing cost to reach the domain
- The input ports routed through the output port

The FSPF protocol supports equal cost multipaths, so there could be multiple parallel paths between two switches.

The command syntax is topologyShow to list all domains.

```
admin> topologyShow

Local Domain ID: 1

Domain  Metric    Hops    Out Port   In Port      Flags    Name
--------------------------------------------------------------------------
   1    2000       2         2      0x00000050    D     "open348"
                   2         1      0x00000020    D
                   2         0      0x00000080    D

Type <CR> to continue, Q<CR> to stop:

   4    3000       3         2      0x00000050    D     "open375"
                   3         1      0x00000020    D
                   3         0      0x00000080    D

Type <CR> to continue, Q<CR> to stop: q
```

Figure A-102. topologyShow command example 1

The command syntax is topologyShow <domain ID> to list a specified domain.

```
admin> topologyShow 1

Local Domain ID: 1

Domain  Metric    Hops    Out Port   In Port      Flags    Name
--------------------------------------------------------------------------
   1    2000       2         2      0x00000050    D     "open148"
                   2         1      0x00000020    D
                   2         0      0x00000080    D
```

Figure A-103. topologyShow command example 2

Table A-28
topologyShow Command Field Descriptions

Field	Description
Domain	The destination domain
Metric	The total cost to reach the destination domain, or the sum of all link costs traversed by a frame to reach the destination domain. A metric of 1000 indicates the destination domain is one hop away from the local switch, since 1000 is the cost of a 1 Gbps link.
Hops	The number of hops (switches) between the local and remote switches.
Out Port	The out port used to route frames to the domain.

continued

Table A-28
topologyShow Command Field Descriptions *continued*

Field	Description
In Port	A bitmap field that indicates which ports are routed through the out port to reach the destination domain.
Flags	Indicates how the switch acquired this path. Possible values are: D—The path was dynamically discovered by the FSPF protocol. S—The path was statically configured through the shell.
Name	The switch name in the domain.

uRouteConfig

Figure A-104 shows the uRouteConfig command, which lets you select the destination traffic's path on a source-port basis. The command syntax is:

uRouteConfig <port>, <domain>, <output port>

After using this command, traffic coming in from the port addressed to a domain is forwarded through the output port. Make sure that the output port is a viable path for reaching the domain. The port can be an E-Port or an F_Port. If it is an E_Port, make sure that no routing loops are created.

If the output is not an E_Port, the route is allocated dynamically to a different path, if one is available, as if this was a regular route. If the output port goes down, the route is treated as a regular route and is allocated to a different path if one is available. When the output port comes back up, the port is rerouted back to the static route.

Load sharing continues, taking into account static routes when counting the number of routes that are allocated to a path, acting only on regular, non-static routes.

If the port has a static route, the flags field in uRouteShow is set to S instead of D. This does not affect the flags field in the topologyShow command. The topologyShow command still shows D unless a static path is configured.

```
switch:admin>uRouteConfig 2,2,4
committing configuration...done.
```

Figure A-104. uRouteConfig command example

uRouteRemove

Figure A-105 shows the uRouteRemove command, which removes the static route configured by the uRouteConfig command.

```
switch:admin>uRouteRemove 2,2
committing configuration...done.
```

Figure A-105. uRouteRemove command example

uRouteShow

Figure A-106 shows the uRouteShow command, which displays the port's unicast routing information (the output port used to forward frames from a port to the domain). Only one output port is used to forward frames from one input port to a destination domain.

The command uRouteShow has three syntax options:

- uRouteShow <port #> <domain ID>—Displays the route for port <port #> to a specific domain <domain ID>
- uRouteShow <port #>—Displays the route for port <port #> to all of the active domains in the fabric
- uRouteShow—Displays the route for all of the ports on the switch to all the active domains in the fabric

For all three formats, uRouteShow displays the domain ID of the next hop and the port number on the next hop for each route.

```
admin> uRouteShow

Local Domain ID: 1

In Port  Domain  Out Port  Metric   Hops  Flags  Next(Dom,Port)
------------------------------------------------------------------
   0       5        7      1000     1     D        5,6
           6        7      2000     2     D        5,6
           7        7      3000     3     D        5,6
           8        7      4000     4     D        5,6
           9        7      5000     5     D        5,6

1          5        5      1000     1     D        5,5
           6        5      2000     2     D        5,5
           7        5      3000     3     D        5,5
           8        5      4000     4     D        5,5
           9        5      5000     5     D        5,5

2          5        4      1000     1     D        5,4
           6        4      2000     2     D        5,4
           7        4      3000     3     D        5,4
           8        4      4000     4     D        5,4
           9        4      5000     5     D        5,4
```

Figure A-106. uRouteShow command example

Table A-29
uRouteShow Command Field Descriptions

Field	Description
In Port	A bitmap field that indicates what ports are routed through the out port to reach the destination domain
Domain	The destination domain
Out Port	The out ports used to route frames to the domain
Metric	The total cost to reach the destination domain, or the sum of all link costs traversed by a frame to reach the destination domain. A metric of 1000 indicates the destination domain is one hop away from the local switch, since 1000 is the cost of a 1 Gbps link.
Hops	The number of hops (switches) between the local and remote switches
Flags	Indicates how the switch acquired this path. Possible values are: D—The path was dynamically discovered by the FSPF protocol. S—The path was statically configured through the shell.
Next (Dom, Port)	The domain ID that the remote switch (out port) is connected to, and the port ID on the remote switch.

License Commands

License commands let you view, add, and remove license keys.

licenseAdd

Figure A-107 shows the licenseAdd command, which adds licenses. Licenses can be checked using the licenseShow command.

```
admin> licenseAdd "342kj4324KJ23423dn"
```

Figure A-107. licenseAdd command example

licenseRemove

Figure A-108 shows the licenseRemove command, which deletes licensed products. The value returned depends on the license keys removed. Check remaining licenses with the licenseShow command.

```
admin> licenseRemove "342kj4324KJ23423dn"
```

Figure A-108. licenseRemove command example

licenseShow

Figure A-109 shows the licenseShow command, which displays the optionally licensed products installed on the SAN Switch. The value returned depends on the license keys installed. If no optional software features have been added, no value is returned.

NOTE: If the switch does not have a Fabric Operating System license installed, the licenseShow command only returns Web Management Tools. QuickLoop functionality is the default state if a Fabric Operating System license is not installed.

```
admin> licenseShow

Webtools

Zoning
```

Figure A-109. licenseShow command example

Zoning-Specific Telnet Commands

Zoning-specific Telnet commands can be used when you do not have access to the Web interface. This section contains information and examples on managing zones using:

- Zone alias commands
- Zone configuration commands
- Zone commands
- Configuration management commands

The Zoning commands are added to switch's admin account to manage zone aliases, zone configurations, and zones.

All add, create, delete, and remove commands modify the defined configuration. This has no effect on the effective configuration until you execute a cfgEnable command. Table A-30 summarizes the commands.

Table A-30
Zoning Commands

Command Type	Command
Zone alias	aliAdd
	aliCreate
	aliDelete
	aliRemove
	aliShow
Zone configuration	cfgAdd
	cfgCreate
	cfgDelete
	cfgRemove
	cfgShow

continued

Table A-30
Zoning Commands *continued*

Command Type	Command
Zone	zoneAdd
	zoneCreate
	zoneDelete
	zoneRemove
	zoneShow
Configuration management	cfgClear
	cfgDisable
	cfgEnable
	cfgSave

Zone Alias Commands

Zone alias commands let you manipulate the zone aliases. Table A-31 summarizes the commands.

Table A-31
Zone Alias Command Descriptions

Command	Description
aliAdd	Adds a member to a zone alias
aliCreate	Creates a zone alias
aliDelete	Deletes a zone alias
aliRemove	Removes a member from a zone alias
aliShow	Shows zone alias definition

aliAdd

Figure A-110 shows the aliAdd command, which adds one or more new alias members to an existing zone alias. The alias members list contains one or more physical fabric port numbers or WWNs, separated by semicolons. The alias members list cannot contain other zone aliases.

```
admin> aliAdd "array1", "21:00:00:20:37:0c:72:51;
21:00:00:20:37:0c:71:0a"
admin> aliAdd "array2", "21:00:00:20:37:0c:9c:6b;
21:00:00:20:37:0c:66:3a"
admin> aliAdd "loop1", "21:00:00:20:37:0c:6a:40;
21:00:00:20:37:0c:59:7e"
```

Figure A-110. aliAdd command example

aliCreate

Figure A-111 shows the aliCreate command, which creates a new zone alias. The alias name cannot be used for any other zone object.

```
admin> aliCreate "array1", "21:00:00:20:37:0c:76:8c;
21:00:00:20:37:0c:71:d2"
admin> aliCreate "array2", "21:00:00:20:37:0c:66:23;
21:00:00:20:37:0c:73:7f"
admin> aliCreate "loop1", "21:00:00:20:37:0c:67:e3;
21:00:00:20:37:0c:76:1f"
```

Figure A-111. aliCreate command example

aliDelete

Figure A-112 shows the aliDelete command, which deletes an existing zone alias.

```
admin> aliDelete "array2"
```

Figure A-112. aliDelete command example

aliRemove

Figure A-113 shows the aliRemove command, which removes one or more alias members from an existing zone alias. An exact string match removes the members. If executing this command results in all members being removed, the zone alias is deleted.

```
admin> aliRemove "array1", "21:00:00:20:37:0c:71:d2"
```

Figure A-113. aliRemove command example

aliShow

Figure A-114 shows the aliShow command, which shows the specified zone alias definition if a parameter is given. If no parameter is given, all zone configuration information is shown.

```
admin> aliShow
Defined configuration:
  cfg:    USA_cfg Red_zone; Blue_zone
  zone:  Blue_zone
                  0,1; array1; 0,2; array2
  zone:  Red_zone
                  0,0; loop1
  alias:  array1    21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
  alias:  array2    21:00:00:20:37:0c:66:23; 21:00:00:20:37:0c:73:7f
  alias:  loop1     21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
  no configuration in effect
```

Figure A-114. aliShow command example

Zone Configuration Commands

Zone configuration commands let you manipulate the zone configurations. Table A-32 summarizes the commands.

Table A-32
Zone Configuration Command Descriptions

Command	Description
cfgAdd	Adds a zone to a configuration
cfgCreate	Creates a zone configuration
cfgDelete	Deletes a zone configuration
cfgRemove	Removes a zone from a configuration
cfgShow	Shows a zone configuration definition

cfgAdd

Figure A-115 shows the cfgAdd command, which adds one or more new members to an existing zone configuration.

```
admin> cfgAdd "USA_cfg", "Green_zone"
```

Figure A-115. cfgAdd command example

cfgCreate

Figure A-116 shows the cfgCreate command, which creates a new zone configuration. The name used for the zone configuration cannot be used for any other zone object. The members list contains one or more zone names, separated by semicolons. White space is ignored.

```
admin> cfgCreate "USA_cfg", "Red_zone; Blue_zone; Green_zone"
```

Figure A-116. cfgCreate command example

cfgDelete

Figure A-117 shows the cfgDelete command, which deletes an existing zone configuration.

```
admin> cfgDelete "USA_cfg"
```

Figure A-117. cfgDelete command example

cfgRemove

Figure A-118 shows the cfgRemove command, which removes one or more members from an existing zone configuration. An exact string match removes the members. If executing this command results in all members being removed, the zone configuration is deleted.

```
admin> cfgRemove "USA_cfg", "Green_zone"
```

Figure A-118. cfgRemove command example

cfgShow

Figure A-119 shows the cfgShow command, which shows the specified zone configuration definition if a parameter is given. If no parameter is given, all zone configuration information is shown.

```
admin> cfgShow
Defined configuration:
 cfg:    USA_cfg Red_zone; Blue_zone; Green_zone
 zone:  Blue_zone
                 0,1; array1; 0,2; array2
 zone:  Red_zone
                 0,0; loop1
 alias:  array1    21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
 alias:  array2    21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
 alias:  loop1     21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
 cfg:    USA_cfg
 zone:  Blue_zone
                 0,1
                 21:00:00:20:37:0c:76:8c
                 21:00:00:20:37:0c:71:02
                 0,2
                 21:00:00:20:37:0c:76:22
                 21:00:00:20:37:0c:76:28
 zone:  Red_zone
                 0,0
                 21:00:00:20:37:0c:76:85
                 21:00:00:20:37:0c:71:df
```

Figure A-119. cfgShow command example

Zone Commands

Zone commands let you manipulate the zones within a fabric. Table A-33 summarizes the commands.

Table A-33
Zone Command Descriptions

Command	Description
zoneAdd	Adds a member to a zone
zoneCreate	Creates a zone
zoneDelete	Deletes a zone
zoneRemove	Removes a member from a zone
zoneShow	Shows a zone definition

zoneAdd

Figure A-120 shows the zoneAdd command, which adds one or more new zone members to an existing zone.

```
admin> zoneAdd "Blue_zone", "array2"
```

Figure A-120. zoneAdd command example

zoneCreate

Figure A-121 shows the zoneCreate command, which creates a new zone. The zone name cannot be used for any other zone object. The zone members list contains one or more physical fabric port numbers, WWNs, or zone alias names, separated by semicolons. White space is ignored.

```
admin> zoneCreate "Red_zone", "0,0; loop1"
admin> zoneCreate "Blue_zone", "0,1; array1; 0,2; array2"
admin> zoneCreate "Green_zone", "0,0; loop1; 0,2; array2"
```

Figure A-121. zoneCreate command example

zoneDelete

Figure A-122 shows the zoneDelete command, which deletes an existing zone.

```
admin> zoneDelete "Blue_zone"
```

Figure A-122. zoneDelete command example

zoneRemove

Figure A-123 shows the zoneRemove command, which removes one or more zone members from an existing zone. An exact string match removes the members. If all zone members are removed, the zone is deleted.

```
admin> zoneRemove "Blue_zone", "array2"
```

Figure A-123. zoneRemove command example

zoneShow

Figure A-124 shows the zoneShow command, which shows the specified zone definition if a parameter is given. If no parameter is given, all zone configuration information is shown.

```
admin> zoneShow
Defined configuration:
  cfg:    USA_cfg Red_zone; Blue_zone; Green_zone
  zone:  Blue_zone
                  0,1; array1; 0,2; array2
  zone:  Red_zone
                  0,0; loop1
  alias:  array1    21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
  alias:  array2    21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
  alias:  loop1     21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df
Effective configuration:
  cfg:    USA_cfg
  zone:  Blue_zone
                  0,1
                  21:00:00:20:37:0c:76:8c
                  21:00:00:20:37:0c:71:02
                  0,2
                  21:00:00:20:37:0c:76:22
                  21:00:00:20:37:0c:76:28
  zone:    Red_zone
                  0,0
                  21:00:00:20:37:0c:76:85
                  21:00:00:20:37:0c:71:df
```

Figure A-124. zoneShow command example

Configuration Management Commands

Configuration management commands let you configure the zones. Table A-34 summarizes the commands.

Table A-34
Configuration Management Command Descriptions

Command	Description
cfgClear	Clears all zone configurations
cfgDisable	Disables a zone configuration
cfgEnable	Enables a zone configuration
cfgSave	Saves zone configurations in flash

cfgClear

Figure A-125 shows the cfgClear command, which should be used with caution. If a zone configuration is enabled, this command disables it, deletes all zone components, and erases the zone configuration stored in flash memory. After you execute this command, no zone information remains in the fabric.

CAUTION: Use of this command removes all zone information from the fabric.

```
admin> cfgClear
```

Figure A-125. cfgClear command example

cfgDisable

Figure A-126 shows the cfgDisable command, which disables the current zone configuration. The fabric returns to non-zoning mode, where all devices can access each other.

```
admin> cfgDisable "USA_cfg"
```

Figure A-126. cfgDisable command example

cfgEnable

Figure A-127 shows the cfgEnable command. The specified zone configuration is compiled after checking for undefined zone names, zone alias names, or other inconsistencies by expanding zone aliases, removing duplicate entries, and then building the effective configuration. If the compilation fails, the previous state is unchanged. If the compilation succeeds, the previous effective configuration is disabled and the new configuration is installed and enabled.

```
admin> cfgEnable "USA_cfg"
zone config "USA_cfg" is in effect
```

Figure A-127. cfgEnable command example

cfgSave

Figure A-128 shows the cfgSave command, which writes a copy of the defined configuration, the name of the effective configuration, and the state of the configuration (enabled or disabled) to flash memory in all fabric switches. When the system is powering up, the switch automatically reloads the most recent saved configuration.

```
admin> cfgSave
Updating flash ...
```

Figure A-128. cfgSave command example

Glossary

Alias Server

An Alias Server is a fabric software facility that supports multicast group management.

Arbitrated Loop

The Fibre Channel Arbitrated Loop (FC-AL) is a loop where several Fibre Channel nodes arbitrate for access to a shared common medium.

Community

An SNMP community is a relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

Credit

Credit is a numeric value applied to a switch. The value represents the maximum number of receive buffers provided by an F_Port or FL_Port to its attached N_Port or NL_Port, respectively, such that the N_Port or NL_Port can transmit frames without over-running the F_Port or NL_Port.

Class 2

In Class 2 service, the fabric and destination N_Port provide connectionless service with notification of delivery or nondelivery between the two N_Ports.

Class 3

Class 3 service provides a connectionless service without notification of delivery between N_Ports. The transmission and routing of Class 3 frames is the same as for Class 2 frames.

Domain ID

The domain number uniquely identifies a switch in a fabric. Normally, the switch automatically assigns the domain ID. The domain ID can be any value between 0 and 31 for version 1.06 firmware and between 1 and 239 for firmware version 2.03a and later.

E_Port

An E_Port is used as an interswitch expansion port. It connects to the E_Port of another switch to build a larger fabric.

Error Detect Time Out Value

The Error-Detect Time-Out Value (E_D_TOV) is equal to the time the switch waits for an expected response before declaring an error condition.

Fabric

A fabric is a network comprised of high-speed fiber connections resulting from the interconnection of switches and devices. A fabric is an active and intelligent nonshared interconnect scheme for nodes.

FL_Port

An FL_Port is a fabric access port used to connect NL_Ports to the switch in a loop configuration.

F_Port

An F_Port is a fabric access port used to connect an N_Port.

Giga Bit Interface Converter module

A Giga Bit Interface Converter (GBIC) module is a removable serial transceiver designed to provide gigabaud capability for Fibre Channel and other protocols that use the same physical layer.

G_Port

A G_Port is a generic switch port that can operate either as an E_Port or as an F_Port.

Interswitch Link

The Interswitch Link (ISL) is a fiber link between two switches.

Isolated E_Port

An E_Port is isolated when the ISL is online but not operational between switches because of overlapping domain ID or nonidentical parameters such as E_D_TOVs or zone configuration definitions.

Loop

A loop is a configuration of devices connected to the fabric by way of a U_Port interface card that is in FL_Port mode.

Multicast

Multicast is used when multiple copies of data are to be sent to designated multiple destinations.

N_Port

An N_Port is an equipment port connected to the fabric.

NL_Port

An NL_Port is an equipment port connected to the fabric in a loop configuration by way of an FL_Port.

Power On Self-Test

The Power On Self-Test (POST) is a series of self-tests that run each time the switch is booted or reset.

Resource Allocation Time Out Value

The Resource Allocation Time Out Value (R_A_TOV) is used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a TCP/IP protocol that generally uses the User Datagram Protocol (UDP) to exchange messages between a management information base and a management client residing on a network. Since SNMP does not rely on the underlying communication protocols, it can be made available over other protocols, such as UDP/IP.

SNMPv1

The original standard for SNMP is now referred to as SNMPv1.

Tachyon

Tachyon refers to a Fibre Channel controller that focuses on arbitrated loop topologies for cost-effective Fibre Channel mass storage designs. Tachyon family architecture is a complete hardware-based design that delivers on the true performance capabilities of Fibre Channel.

Trap

An SNMP trap is a mechanism for SNMP agents to notify the SNMP management station of significant events.

Unicast

Unicast routing provides one or more optimal paths between any two switches that make up the fabric. This allows for a single copy of data to be sent to designated destinations.

U-Port

A U_Port is a generic switch port that can operate either as an E_Port, F_Port, or FL_Port. A port is defined as a U_Port, for example, when it is not connected or has not yet assumed a specific function in the fabric.

World Wide Name

A World Wide Name (WWN) uniquely identifies a switch on local and global networks.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z