Cisco SFS Product Family Element Manager User Guide

Release 2.9.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-9161-04

Cisco SFS Product Family Element Manager User Guide

CONTENTS

Preface

This preface describes who should read the *Cisco SFS Product Family Element Manager User Guide*, how it is organized, and its document conventions. It contains the following sections:

Audience

The intended audience is the administrator responsible for installing, configuring, and managing InfiniBand switch equipment. This administrator should have experience administering similar networking or storage equipment.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	About Element Manager	Describes Element Manager fundamentals.
Chapter 2	Chassis Display Tasks	Describes tasks you can perform on the chassis display.
Chapter 3	File Tasks	Describes tasks you can perform on the file menu display.
Chapter 4	Edit Tasks	Describes tasks you can perform on the edit menu display.
Chapter 5	Maintenance Tasks	Describes tasks you can perform on the maintenance menu display.
Chapter 6	Health Tasks	Describes tasks you can perform on the health menu display.

Chapter	Title	Description
Chapter 7	Report Tasks	Describes tasks you can perform on the report menu display.
Chapter 8	InfiniBand Subnet Management Tasks	Describes the subnet management tasks you can perform on the InfiniBand menu display.
Chapter 9	InfiniBand Performance Management Tasks	Describes the performance management tasks you can perform on the InfiniBand menu display.
Chapter 10	InfiniBand Topology View Tasks	Describes how to use the Topology view from the InfiniBand menu display.
Chapter 11	InfiniBand Device Management Tasks	Describes InfiniBand device management tasks you can perform from the InfiniBand menu display.
Chapter 12	Ethernet Menu Tasks	Describes tasks you can perform on the Ethernet menu display.
Chapter 13	FibreChannel Menu Tasks	Describes tasks you can perform on the fibre channel menu display.
Chapter 14	Help Menu Tasks	Describes tasks you can perform on the help menu display.
Appendix A	InfiniBand Concepts	Provides conceptual information about InfiniBand entities.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**. Bold text indicates Chassis Manager elements or text that you must enter as-is.
italic font	Arguments in commands for which you supply values are in *italics*. Italics not used in commands indicate emphasis.
Menu1 > Menu2 > Item…	Series indicate a pop-up menu sequence to open a form or execute a desired function.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or arguments; for example, {**interface** *interface* **type**}.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Convention	Description
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For additional information about Cisco SFS switches and command-line interface (CLI) commands, see the following documentation:

- *Release Notes for Cisco SFS 7000D Series Switch Software Release 2.9.0*
- *Cisco SFS Product Family Chassis Manager User Guide*
- *Cisco SFS Product Family Command Reference*

For detailed hardware configuration and maintenance procedures, see these hardware guides:

- *Cisco SFS 7000P InfiniBand Server Switch Installation and Configuration Note*
- *Cisco SFS 7008P InfiniBand Server Switch Installation and Configuration Note*
- *Cisco SFS 7008P InfiniBand Server Hardware Installation Guide*
- *Cisco SFS 7000D InfiniBand Server Switch Installation and Configuration Note*
- *Cisco SFS 7000P and SFS 7000D InfiniBand Server Switches Hardware Installation Guide*
- *Cisco SFS 3012R Multifabric Server Switch Installation and Configuration Note*
- *Cisco SFS 3012R Multifabric Server Switch Hardware Installation Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

About Element Manager

These topics describe the Element Manager Java-based user-interface (GUI) that runs on your server switch:

Introduction

With Element Manager, you can manage individual server switches from an easy-to-use GUI. To run Element Manager, you must complete the following tasks:

- Install the Element Manager software on a host or workstation.
- Configure your server switches to support Element Manager.
- Launch Element Manager on your host or workstation.

The following topics describe basic features of the Element Manager user interface:

Element Manager Primary Display

The primary display of Element Manager provides drop-down menus, feature buttons, and various clickable display elements. Figure 1-1 shows the Element Manager display.

Figure 1-1 Element Manager Primary Display

The number of menus, icons, and display elements vary by server switch platform. Table 1-1 and Table 1-2 list and describe all possible menus and buttons. Clickable display elements vary by hardware platform.

When you click a display element (such as server switch ports), a yellow border appears around the element. You can double-click any clickable element to open a related configuration window. You can right-click these elements to view element-specific menus. You can use these menus and windows to view element details or change the configuration.

You can press the **Ctrl** key and click multiple elements of the same type (for instance, multiple InfiniBand ports) to select multiple elements at once to configure them as a group. After you select multiple elements, right-click one of the elements to display a right-click menu for options that you can apply.

Element Manager Menus

Table 1-1 describes the drop-down menus in the Element Manager display.

Table 1-1 Element Manager Drop-down Menus

Menu	Description
File	Use the menu items in the File menu to do the following: • Load a server switch in the Element Manager display. • Configure performance options such as intervals and thresholds for various features. • Refresh the display. • Telnet to the open server switch to configure the switch with the command-line interface (CLI). (For CLI details, see the *Cisco SFS Product Family Command Reference*.)
Edit	Use the Edit menu to view port properties or card properties.

Table 1-1 Element Manager Drop-down Menus (continued)

Menu	Description
Maintenance	Use the menu items in the Maintenance menu to do the following: • View server switch details. • View and configure basic services. • View and configure the boot configuration. • Back up the running configuration. • Import and export files. • Reboot the server switch. • Track diagnostic tests.
Health	Use the menu items in the Health menu to monitor the server switch status and events.
Report	Use the menu items in the Report menu to graph server switch statistics.
InfiniBand	Use the menu items in the InfiniBand menu to configure InfiniBand-specific server switch features, including the Device Manager and Subnet Manager.
Ethernet	Use the menu items in the Ethernet menu to configure Ethernet-specific server switch features.
Fibre Channel	Use the menu items in the Fibre Channel menu to configure Fibre Channel-specific server switch features.
Help	Use the menu items in the Help menu to launch the online help and locate additional help resources.

Element Manager Icons

Table 1-2 describes the feature icons in the Element Manager display.

Table 1-2 Element Manager Feature Icons

Icon	Description
	Click **Open** to load a different server switch in the display.
	Click **Refresh** to poll the server switch and update the display.
	Click **Telnet** to launch a Telnet session to the server switch.
	Click **Help** to launch the online help.
	Click **Properties** after you click an element (or multiple elements of the same type) to view the properties of the element(s).
	Click **Graph** after you click an element (or multiple elements of the same type) to select element statistics that you can then graph.

Table 1-2 Element Manager Feature Icons (continued)

Icon	Description
	Click **Topology** to view the server switch and neighboring devices.
	Click **Subnet Management** to open the Subnet Management window and configure partitions, multicast groups, and other Subnet Manager-related features.
	Click **Storage Manager** to open the Storage Manager window and configure initiators, targets, and LUNs.

Common GUI Buttons

Many windows that you can open in Element Manager display a combination of frequently appearing buttons. Table 1-3 describes these common buttons.

Table 1-3 Common Buttons

Button	Description
Apply	Applies any changes that you made in the window to the server switch.
Refresh	Updates the window with the latest information from the server switch.
Close	Closes the window.
Help	Launches the online help.

Status Indicators

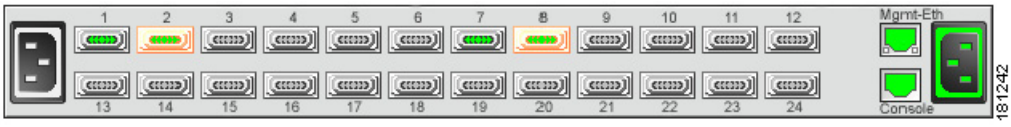
The Element Manager display uses specific colors to communicate the status of server switch elements. Table 1-4 describes status-indicator colors.

Table 1-4 Status Indicator Colors

Color	Indication
gray	Element is not active (such as an InfiniBand port that does not connect to a cable).
red	An administrator has taken the element offline or the element experiences an error.
green	Element functions successfully.
transparent	Element is unmanaged.

Color is also used on the primary display to indicate not only the up/down status of ports, but also the configured lane width of InfiniBand ports, as shown in Figure 1-2.

Figure 1-2 Primary View Showing Port Status



Ports 1 through 24 are InfiniBand ports.

- Ports with an operational status of up show with green pins.
- InfiniBand ports configured with double data rate (DDR) operational speed show with green pins and an orange surround.
- InfiniBand ports configured with single data rate (SDR) operational speed appear with green pins and a grey surround.

Installing Element Manager

Element Manager runs on Linux, Solaris, and Windows platforms. Follow installation instructions for the appropriate platform:

- System Requirements (All Platforms), page 1-5
- Linux Installation, page 1-5
- Solaris Installation, page 1-6
- Windows Installation, page 1-6

System Requirements (All Platforms)

To install Element Manager, your system must meet the following requirements:

- 64 MB of available RAM
- 75 MB of available hard disk space and 50 MB of additional available hard disk space during installation
- 300-MHz processor
- 800 x 600 screen resolution with 16-bit color depth

Linux Installation

To install Element Manager on Linux, follow these steps:

Step 1 Log in to your Linux host.

Step 2 Download the Element Manager software from the Cisco Software Download Center:

http://www.cisco.com/public/sw-center/

Step 3 Navigate to the Linux directory of the downloaded software.

Step 4 Run the appropriate binary file, and proceed with the installation wizard.

Solaris Installation

To install Element Manager on Solaris, follow these steps:

Step 1 Log in to your Solaris host.

Step 2 Download the Element Manager software from the Cisco Software Download Center:

http://www.cisco.com/public/sw-center/

Step 3 Navigate to the em/Solaris directory of the downloaded software.

Step 4 Start the **./install_*yourOS*.bin** file. Proceed with the installation wizard.

Windows Installation

To install Element Manager on Windows, follow these steps:

Step 1 Log in to your Windows host.

Step 2 Download the Element Manager software from the Cisco Software Download Center:

http://www.cisco.com/public/sw-center/

Step 3 Navigate to the Windows directory of the downloaded software.

Step 4 Launch the executable file (em.exe) to begin the installation process.

The Introduction screen appears.

Step 5 Click **Next**.

The License Agreement screen appears.

Step 6 Read the license agreement, choose **I accept the terms of the license agreement**, and then click **Next**.

The Choose Install Folder screen appears.

Step 7 Select a folder, and then click **Next**.

The Choose Shortcut Folder screen appears.

Step 8 Make selections as appropriate for your needs, and then click **Next**.

The Pre-Installation Summary screen appears.

Step 9 Verify installation information in the Please Review the Following Before Continuing window, and then click **Install**.

The installation executes.

Step 10 Click **Done** when the installation completes.

Launching Element Manager

When you launch Element Manager, the interface requests the IP address (or DNS name) of the server switch that you want to manage. To successfully connect to the server switch that you want to manage, you must first configure that server switch to permit Element Manager access. If Element Manager fails to connect to a given server switch, verify that the server switch meets the prerequisites for Element Manager. See the "Preparing Your Server Switch" section on page 1-7.

Preparing Your Server Switch

Factory defaults permit your server switch to connect to Element Manager. The following settings must apply to your server switch to open in Element Manager:

- HTTP server enabled
- Telnet server enabled
- SNMP server configured

To view your server switch settings, follow these steps:

Step 1 Log in to your server switch.

Step 2 Enter the **enable** command to enter privileged EXEC mode.

Step 3 Enter the **configure terminal** command to enter global configuration mode.

Step 4 Enter the **ip http server** command to enable the HTTP server.

Step 5 Enter the Telnet **enable** command to enable Telnet services.

Step 6 To configure the SNMP server, enter the **snmp-server** command with the following:

- IP address of the server that you want to configure
- (Optional) **recv-event-traps** keyword

For more information, see the *Cisco SFS Product Family Command Reference*.

CHAPTER 2

Chassis Display Tasks

These topics describe the chassis display tasks for Element Manager:

Note When you launch Element Manager and open a server switch, a graphical display of that server switch appears. Colors in the display indicate the status of various components of the server switch. Various right- and left-click options let you configure the components that you see in the display.

Viewing Card Properties

To view card properties, follow these steps:

Step 1 Right-click the card in the chassis display with properties that you want to view.

A right-click menu appears.

Step 2 From the right-click menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar. Table 2-1 describes the fields that appear in the Card tab of the card window.

Table 2-1 Card Tab Fields

Field	Description
Admin Type (gateway cards only)	Administratively configured card type.
Card Type field	Dynamically discovered card type.
Enable/Disable Card (choose cards only)	Up and down radio buttons enable or disable the card.
Current Card Status	Displays up if the card can currently run traffic; otherwise, displays down.
Operational State	Displays the general condition of the interface card. The general condition can be any of the following: • unknown • normal • wrongBootImage • bootFailed • tooHot • booting A condition of unknown indicates an unsupported interface card. To address this condition, replace the card with a supported card. The operational state of a card must be normal for the current status of the card to appear as up. A wrong-image condition indicates that the active system image on the interface card does not match the active system image on the controller. All cards must run the same active system image as the controller card. A bootFailed condition indicates that the active system image on the card was incompletely or incorrectly loaded. If the other interface cards come up successfully, reset the individual card; otherwise, reboot your entire device. A tooHot condition indicates that the card is overheating. From the Health menu, click **Status** and then select the **Fans** tab to see if your fans failed. The booting condition indicates that the card has not finished loading the necessary image data for internal configuration.

Table 2-1 Card Tab Fields (continued)

Field	Description
Card Boot Stage	Boot Stage values can be any of the following: • recovery • ipl • ppcboot • fpga • pic • ib • rootfs • kernel • exe • done • none
Card Boot Status	Boot Status values can be any of the following: • upgrading • success • failed • badVersion • badCrc • memoryError • outOfSpace • programmingError • hardwareError • fileNotFound • inProgress • none
Serial Number	Factory-assigned product serial number of the card.
PCA Serial Number	Printed circuit assembly (PCA) serial number of the card.
PCA Assembly Number	Printed circuit assembly (PCA) assembly number of the card.
FRU Number	Field-replaceable unit (FRU) number of the card.
Product Version ID	Version of the product.
Action (varies by card type)	Provides none, reset, and deleteInactiveImages radio buttons. For more information, see the "Deleting Inactive Images from an Interface Card" section on page 2-4 and the "Resetting an Interface Card" section on page 2-4.
Result	Result of the action from the Action field.

Deleting Inactive Images from an Interface Card

To remove an inactive image from an interface card, follow these steps:

Step 1 Right-click the card in the chassis display with properties that you want to view.

A menu appears.

Step 2 From the menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 In the Action field, click the **deleteInactiveImages** radio button.

Step 4 Click **Apply**.

Resetting an Interface Card

To reset an interface card, follow these steps:

Step 1 Right-click the card in the chassis display with properties that you want to reset.

A menu appears.

Step 2 From the menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 In the Action field, click the **reset** radio button.

Step 4 Click **Apply**.

Enabling or Disabling a Card

With Element Manager, you can bring up or shut down any card on your chassis. These procedures configure the administrative status of a card:

- Enabling a Card, page 2-4
- Disabling a Card, page 2-5

Enabling a Card

To enable an interface card, follow these steps:

Step 1 Right-click the card in the chassis display that you want to bring up.

A menu appears.

Step 2 From the menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 In the Enable/Disable Card field, click the **up** radio button.

Step 4 Click **Apply**.

Disabling a Card

To disable a card, follow these steps:

Step 1 Right-click the card in the chassis display that you want to shut down.

A menu appears.

Step 2 From the menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 In the Enable/Disable Card field, click the **down** radio button.

Step 4 Click **Apply**.

Viewing the Card Inventory

To view memory and image information on a card, follow these steps:

Step 1 Right-click the card in the chassis display with properties that you want to view.

A right-click menu appears.

Step 2 From the right-click menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 Click the **Inventory** tab.

Table 2-2 describes the fields in the Inventory tab of the card window.

Table 2-2 Inventory Tab Field Descriptions

Field	Description
Used Memory	Used memory on the card, in kilobytes.
Free Memory	Available memory on the device, in kilobytes.
Used Disk Space	Used disk space on the card, in kilobytes.
Free Disk Space	Available disk space on the device, in kilobytes.
Current Image Source	Image that the card runs.
Image Source for Next Reboot	Image that the card runs when you reboot.
Image One	First image stored on the card.
Image Two	Second image stored on the card.
CPU Description	Description of the CPU on the card.

Table 2-2 Inventory Tab Field Descriptions (continued)

Field	Description
PIC Firmware Revision field (some cards)	Current PIC firmware version that the card runs.
FPGA Firmware Revision field (some cards)	Current FPGA firmware version that the card runs.
IB Firmware Revision field	Version of InfiniBand firmware on the card. See Note below.
Card Uptime	How long, in seconds, the card has been running.

Note For platforms designed with the InfiniScale III switch chip (7000 and 7008 platforms), the Element Manager displays the device ID and version number of the InfiniBand chip for each card. For platforms using the original InfiniScale switch chip (3001 and 3012 platforms), no parenthetical text appears. The Cisco SFS 3001 and Cisco SFS 3012 chassis run original InfiniScale switch chips. The Cisco SFS 7000 and Cisco SFS 7008 chassis run later versions.

Viewing Internal Gateway Ports of a Card

Ethernet Gateway cards use two internal gateway ports to pass traffic through a server switch. To view gateway port details for Ethernet Gateway cards, follow these steps:

Step 1 Right-click the card in the chassis display with gateway ports you want to view.

A right-click menu appears.

Step 2 From the right-click menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 Click the **Gateway Ports** tab.

Table 2-3 describes the fields in the Gateway Ports tab of the card window.

Table 2-3 Gateway Ports Tab Field Descriptions

Field	Description
IfIndex	Port (interface) number, in slot#/port# format
Port Name	Port name
Port Type	Port type
Current Port Speed	Current speed of the port

Viewing Card IP Addresses

To view the IP addresses of Ethernet Gateway cards, follow these steps:

Step 1 Right-click the card in the chassis display with IP addresses you want to view.

A right-click menu appears.

Step 2 From the right-click menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 Click the **IP Addresses** tab.

Table 2-4 describes the fields in the IP Addresses tab of the card window.

Table 2-4 IP Addresses Tab Field Descriptions

Field	Description
Port	Port number, in card#port# format. A port# of 0 represents the internal gateway port of the interface card.
Address	IP address that you assigned to the port.
Netmask	Subnet mask that you assigned to the port.
BcastAddrFormat	IP broadcast address format that the port uses.
ReasmMaxSize	Size of the largest IP datagram that this port can receive and reassemble from incoming fragmented IP datagrams.
Type	Displays primary or backup to indicate whether the interface card acts as the primary or backup interface for the IP address that appears in the address field.
Status	Displays active or inactive to indicate whether the card actively services IP packets addressed to the IP address in the address field or does not service packets to the specified address.

Viewing Card Bridging Details

To view bridging details for Ethernet Gateway cards, follow these steps:

Step 1 Right-click the card in the chassis display with bridging details you want to view.

A menu appears.

Step 2 From the menu, choose **Properties**.

A window opens and displays the type and number of the card in the title bar.

Step 3 Click the **Bridging** tab.

Table 2-5 describes the fields in the Bridging tab of the card window.

Table 2-5 Bridging Tab Field Descriptions

Field	Description
Port	Port number, in slot#/port# format.
IB P_Key	Partition key that you assigned to the bridge group to which the port belongs.
Bridge Group ID	Bridge group to which the port belongs. Assign the bridge group by choosing **Ethernet > Bridging**. For more information, see the "Creating a Bridge Group" section on page 12-9.

Viewing Port Properties

To view port properties, follow these steps:

Step 1 Right-click the port in the chassis display with properties that you want to view.

Step 2 Choose **Properties**.

A window opens and displays the type and number of the port in the title bar. The contents of the window vary by port type.

- Table 2-6 describes the fields in the properties window of an Ethernet port.
- Table 2-7 describes the fields in the properties window of a Fibre Channel port.
- Table 2-8 describes the fields in the properties window of an InfiniBand port.

Table 2-6 Ethernet Port Properties Window Field Descriptions

Field	Description
Port Type	Identifies the port type based on the function of the port (Ethernet, Fibre Channel, or InfiniBand) and the type of card on which the port resides.
Port Name	A port name that you can edit and apply to the port.

Table 2-6 Ethernet Port Properties Window Field Descriptions (continued)

Field	Description
Enable/Disable Port	Up and down radio buttons let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Physical State	Displays the current state of the port, for example polling.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation	Enables or disables autonegotiation on the port.
Set Port Speed	Radio buttons let you configure the speed of the port.
Current Port Speed	Displays the speed of the port.
Set Duplex (Ethernet gateway ports)	Radio buttons let you configure the duplex setting of the port.
Current Duplex (Ethernet gateway ports)	Indicates whether the port runs in full duplex mode or half duplex mode.
Enable Link Up/Down Trap	Enabled and disabled radio buttons let you configure whether or not the port sends a trap when links go up or down.
MTU	Displays the maximum transmission unit (MTU) of the port, in bytes.
MAC Address	Displays the media access control (MAC) address of the port.
Last Changed On	Displays the time and date of the last time that a user configured the port.
Action (Ethernet gateway ports)	Flushes the ARP table when you choose the **flushArp** radio button, and then click **Apply**. Executes no action if you choose the **none** radio button and click **Apply**.
Result (Ethernet gateway ports)	Displays the result of the action in the Action field after it is applied.

Table 2-7 Fibre Channel Port Properties Window Field Descriptions

Field	Description
Port Type	Identifies the port type based on the function of the port (Ethernet, Fibre Channel, or InfiniBand) and the type of card on which the port resides.
Port Name	Port name that you can edit and apply to the port.
Enable/Disable Port	The up and down radio buttons let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation	Check box lets you enable or disable autonegotiation on the port.
Set Port Speed	Radio buttons let you configure the speed of the port.
Current Port Speed	Displays the speed of the port.

Table 2-7 Fibre Channel Port Properties Window Field Descriptions (continued)

Field	Description
Current Connection Type	Displays the current connection type.
Enable Link Up/Down Trap	Enabled and disabled radio buttons let you configure whether or not the port sends a trap when links go up or down.
MTU	Displays the maximum transmission unit of the port in bytes.
WWNN	World-wide node name of the HCA of the port.
WWPN	World-wide port name of the port.
FC ID	Native Fibre Channel ID of the port.
Last Changed On	Displays the time and date of the last time that a user configured the port.

Table 2-8 InfiniBand Port Properties Window Field Descriptions

Field	Description
Port Type	Identifies the port type based on the function of the port (Ethernet, Fibre Channel, InfiniBand) and the type of card on which the port resides.
Port Name	Port name that you can edit and apply to the port.
Enable/Disable Port	The up and down radio buttons let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Physical State	Displays the current state of the port; for example, polling.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation	Check box lets you enable or disable autonegotiation on the port.
Set Port Speed	Drop-down menu configures the link capacity of the port in terms of its link width (1x, 4x, or 12x) and its lane speed (sdr or ddr). Valid values are 1x-sdr (2.5 Gbps), 4x-sdr (10 Gbps), 12x-sdr(30 Gbps), 1x-ddr (5 Gbps), 4x-ddr (20 Gbps), and 12x-ddr (60 Gbps). **Note** For an InfiniBand port connected with an SDR cable or any cable longer than 8 feet, you must be manually configure the port to support only SDR.
Current Port Speed	Displays the link capacity of the port.
Power Connector Dongle Type	Displays the power connector dongle type only if the port supports the power connector. Possible values are as follows: • none (1) • ib4xFX (2)

Table 2-8 InfiniBand Port Properties Window Field Descriptions (continued)

Field	Description
Power Connector Dongle State	Indicates the power control state of a dongle that is attached to a powered interface connector. Possible values are as follows: • noStateChange (0) • on (1) • off (2)
Clear Counters	Check box lets you clear the port counters.
Enable Link Up/Down Trap	Enabled and disabled radio buttons let you configure whether or not the port sends a trap when links go up or down.
MTU	Displays the maximum transmission unit (MTU) of the port, in bytes.
Last Changed On	Displays the time and date that a user last configured the port.

Viewing Serial Management Port Properties

To view serial management port properties, follow these steps:

Step 1 From the Edit menu, choose **Management Ports**.

The Management Ports window opens.

Step 2 Click the **Serial Port** tab.

Table 2-9 describes the fields in the Serial Port tab.

Table 2-9 Serial Port Field Descriptions

Field	Description
Baud Rate	Baud rate setting to which you must set your serial connection.
Data Bits	Data bit setting to which you must set your serial connection.
Stop Bits	Stop bit setting to which you must set your serial connection.
Parity	Parity field setting to which you must set your serial connection.

If you do not have a serial connection, see the "Establishing a Serial Connection" section on page 2-12.

Establishing a Serial Connection

To create a serial connection to your server switch, follow these steps:

Step 1 Connect the straight-through M/F serial cable (provided with your server switch) to the Serial Management port, and then connect the cable to your terminal, workstation, or terminal server.

Step 2 Launch a terminal session (on a workstation, use a terminal emulation application such as HyperTerminal) and configure your terminal parameters to match the parameters listed in Table 2-9.

Step 3 Press the **Enter** key until the login prompt appears.

Viewing Ethernet Management Port Properties

To view Ethernet management port properties, follow these steps:

Step 1 From the Edit menu, choose **Management Ports**.

The Management Ports window opens.

Step 2 Click the **Ethernet Port** tab.

Table 2-10 describes the fields in the **Ethernet Port** tab.

Table 2-10 Ethernet Management Port Field Descriptions

Field	Description
MAC Address	MAC address of the Ethernet Management Port (which serves as the MAC address of the server switch).
Enable Auto Negotiation	Displays true if the Ethernet Management port dynamically determines the connection speed of the device to which it connects over the Ethernet cable; otherwise, it displays false.
Administrative Port Status	Displays the administrative status that you configure through the CLI with the **shutdown** and **no shutdown** commands.
Current Port Status	Displays up if the port runs successfully. Displays down if the port cannot transmit and receive traffic for any reason.
IP Address	IP address of the Ethernet Management port.
Network Mask	Subnet mask of the Ethernet Management port.
Gateway	Ethernet Gateway assigned to the port.
Address Option	Address option configured with the **addr-option** CLI command.

Viewing and Setting InfiniBand Management Port Properties

These topics discuss viewing and setting InfiniBand management port properties:

Viewing InfiniBand Management Port Properties

To view InfiniBand management port properties, follow these steps:

Step 1 From the Edit menu, and choose **Management Ports**.

The Management Ports window opens.

Step 2 Click the **InfiniBand Port** tab.

Table 2-11 describes the fields in the InfiniBand Port tab.

Table 2-11 InfiniBand Management Port Field Descriptions

Field	Description
Administrative Port Status	Administrative status that you configure through the CLI with the **shutdown** and **no shutdown** commands.
Current Port Status	Displays up if the port runs successfully. Displays down if the port cannot transmit and receive traffic for any reason.
IP Address	IP address of the InfiniBand Management port.
Network Mask	Subnet mask of the InfiniBand Management port.
Gateway	IP address of the gateway that the InfiniBand port uses.
Address Option	Address option configured with the **addr-option** CLI command.
MTU	Maximum transmission unit of the InfiniBand port.

Changing the Inband IPoIB Partition

In case IPoIB multicast joins are disabled on the default partition, you can change the inband IPoIB management partition to a partition that allows IPoIB multicast joins.

To use a different partition as the inband IPoIB management partition, follow these steps:

Step 1 From the Edit menu, choose **Management Ports**.

The Management Ports window opens.

Step 2 Click the **InfiniBand Port** tab.

Step 3 In the PKey field, enter the partition key you want to use for the inband IPoIB partition.

Step 4 Click **Apply**.

Viewing Port Bridging Properties

To view the bridging properties of a port, follow these steps:

Step 1 Right-click the Ethernet port in the chassis display with bridging properties you want to view.

Step 2 From the right-click menu, choose **Properties**.

A window opens and displays the type and number of the port in the title bar. The contents of the window vary by port type.

Step 3 Click the **Bridging** tab.

Table 2-12 describes the fields in this tab.

Table 2-12 Port Bridging Table Field Descriptions

Field	Description
Port	Port that you choose from the Ports table.
IEEE VLAN Tag	Virtual LAN (VLAN) of the bridge to which the port belongs.
Bridge Group ID	Bridge ID of the bridge to which the port belongs.

Configuring Ports

Element Manager provides different configuration options for each type of port. The options available to each port appear in the Port Properties window.

Note To configure multiple ports at once, press the **Ctrl** key and click multiple ports of the same type, and then right-click one of the ports that you selected to view right-click menu options.

These topics describe how to configure port properties:

- Configuring a Port Name, page 2-15
- Enabling or Disabling a Port, page 2-15
- Configuring Autonegotiation on a Port, page 2-15
- Configuring Port Speed, page 2-16
- Clearing InfiniBand Port Counters, page 2-16
- Configuring Port IP Addresses, page 2-16

Configuring a Port Name

To configure the administrative name of a port, follow these steps:

Step 1 Double-click the port that you want to configure.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 In the Port Name field of the window, enter a name for the port, and then click **Apply**.

Step 3 Click **Close** to close the window.

Enabling or Disabling a Port

To enable or disable a port, follow these steps:

Step 1 Double-click the port that you want to configure.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 In the Enable/Disable Port field of the window, click the **up** (enable) or **down** (disable) radio button, and then click **Apply**.

Step 3 Click **Close** to close the Port Properties window.

Tip As a shortcut, right-click the port and choose **Enable** or **Disable**.

Configuring Autonegotiation on a Port

To enable or disable autonegotiation on a port, follow these steps:

Step 1 Double-click the port that you want to configure.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 In the Auto Negotiation Supported field of the window, check the **Enable Auto-Negotiation** check box to enable or uncheck to disable it, and then click **Apply**.

Step 3 Click **Close** to close the window.

Configuring Port Speed

Note For an InfiniBand port connected with an SDR cable or any cable longer than 8 feet, you must manually configure the port to support only SDR.

To configure the speed of a port, follow these steps:

Step 1 Double-click the port that you want to configure.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 In the Auto Negotiation field, uncheck the **Enable** check box.

Step 3 In the Set Port Speed field of the window, select a speed as follows:

- For an Ethernet or Fibre Channel port, click a radio button to select a speed.
- For an InfiniBand port, select a speed from the drop-down menu.

Step 4 Click **Apply**.

Step 5 Click **Close** to close the window.

Clearing InfiniBand Port Counters

To clear InfiniBand port counters, follow these steps:

Step 1 Double-click the port for which you want to clear the counters.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 Check the **Clear Counters** check box.

Step 3 Click **Apply**, and then click **Close**.

See Table 7-1 on page 7-2 for descriptions of the counters reset by this procedure.

Configuring Port IP Addresses

To configure an IP address for a port, follow these steps:

Step 1 Double-click the port that you want to configure.

A window opens that identifies the type of the port and the port number (in slot#port# format).

Step 2 Click the **IP Addresses** tab.

Note Before you can manually add IP addresses, you must configure the port for bridging. For more information, see the *Ethernet Gateway User Guide*.

Step 3 Click **Insert**.

The Insert IP Addresses window opens.

Step 4 Enter an IP address and subnet mask, and then click **Insert**.

The address appears in the table under the IP Addresses tab.

Step 5 Click **Close** to close the window.

Rebooting the Server Switch

To reboot the server switch, follow these steps:

Step 1 Right-click the server switch in the chassis display (avoid selectable elements such as ports and cards), and click **Reboot**.

A window opens and prompts you to save configuration changes.

Step 2 Click **Yes** to save configuration changes, or click **No** to discard the changes.

A window opens to verify that you want to reboot.

Step 3 Click **OK** to reboot; otherwise, click **Cancel**.

CHAPTER 3

File Tasks

These topics describe the File tasks for Element Manager:

Note The File menu in the Element Manager GUI provides basic GUI functions and configuration options. Some icons provide the same functions. Where the menu and the icons overlap, the tasks in this chapter describe both options.

Opening a Server Switch with Element Manager

After you launch Element Manager, you can change the server switch that you view and configure with the GUI. You can configure a server switch other than the one that you opened when you launched Element Manager, using one of the following procedures:

Opening a Server Switch from the File Menu

To open a server switch from the File menu, follow these steps:

Step 1 From the File menu, choose **Open**.

The Open Device window opens.

Step 2 In the Device Name or IP Address field, enter the IP address or DNS name (if applicable) of the server switch that you want to open.

Step 3 In the SNMP Community field, enter the SNMP community to which the server switch belongs.

Step 4 Click **Open**.

The server switch loads in the Element Manager GUI.

Opening a Server Switch Using the Open Icon

To open a server switch with the **Open** icon, do the following:

Step 1 Click the **Open** icon ( ).

The Open Device window opens.

Step 2 Enter the IP address or DNS name (if applicable) of the server switch that you want to open in the Device Name or IP Address field.

Step 3 Enter the SNMP community to which the server switch belongs in the SNMP Community field.

Step 4 Click **Open**.

The server switch loads in the Element Manager GUI.

Configuring Polling

These topics describe how to configure the way Element Manager polls the server switch for updates:

Configuring Polling Interval

To configure the frequency with which Element Manager polls the server switch for updates, do the following:

Step 1 From the File menu, choose **Preferences**.

The Preferences window opens.

Step 2 Click the **Polling** tab.

Step 3 In the Status Interval field, enter an integer value to configure the interval, in seconds, at which Element Manager polls the server switch.

Step 4 In the Hotswap Detect every field, enter an integer value to configure the number of status intervals that pass before Element Manager detects removed or replaced hot-swappable hardware components.

Step 5 Check the **Enable** check box, and then click **OK**.

Disabling Polling

When you disable polling, Element Manager refreshes only when you manually refresh the display. (See the "Refreshing the Element Manager Display" section on page 3-5.) To disable polling, do the following:

Step 1 From the File menu, choose **Preferences**.

The Preferences window opens.

Step 2 Click the **Polling** tab.

Step 3 Uncheck the **Enable** check box, and then click **OK**.

Configuring SNMP Preferences

The SNMP preferences that you can configure depend on the application that controls port 162 on the host that runs Element Manager. Server switches send all SNMP traps to port 162. If you run an application other than Element Manager that manages port 162, you must manually register your host in each server switch that you open with Element Manager to send server switch traps to your application. To manually register your host, see the "Configuring Your Host as a Trap Receiver" section on page 6-8.

If Element Manager controls port 162 to receive SNMP traps from the server switch, you can configure host registration and other options. To configure SNMP preferences, do the following:

Step 1 From the File menu, choose **Preferences**.

The Preferences window opens.

Step 2 Click the **SNMP** tab.

Step 3 In the Retry Count field, enter an integer value (from 0 to 5) to specify the maximum number of retries.

Step 4 In the Timeout field, enter an integer value (from 3 to 30) to configure the SNMP timeout interval, in seconds.

Step 5 (Optional) Check the **Trace** check box to begin tracing SNMP traps.

Note You can view the SNMP traps as you trace them with the Trace Log. (See the "Viewing Element Manager Trace Log" section on page 3-4.)

Step 6 (Optional) Check the **Register for Traps** check box to configure Element Manager to automatically add your host to the Trap Receivers table on any server switch that you open in the Element Manager GUI. If another application on your host receives SNMP traps, see the "Configuring Your Host as a Trap Receiver" section on page 6-8 to send server switch traps to that application.

Note When you check the **Register for Traps** check box, Element Manager automatically checks the **Listen for Traps** check box.

Step 7 (Optional) Check the **Listen for Traps** check box to receive SNMP traps from the server switch.

Note If Element Manager does not let you access this check box, uncheck the **Register for Traps** check box.

Step 8 Click **OK**.

Configuring Miscellaneous Trap Preferences

To configure miscellaneous trap preferences, do the following:

Step 1 From the File menu, and choose **Preferences**.

Step 2 Click the **Misc** tab.

Step 3 In the Max Traps in Log field, enter an integer value to limit the number of traps that appear in the log.

Step 4 (Optional) Check the **Confirm row deletion** check box to confirm the row deletion.

Step 5 (Optional) Check the **Save communities in configuration files** check box to save SNMP communities in the configuration file.

Step 6 Click **OK**.

Viewing Element Manager Trace Log

To view the Element Manager trace log, do the following:

Step 1 From the File menu, choose **Preferences**.

Step 2 Click the **SNMP** tab.

Step 3 Check the **Trace** check box to begin tracing SNMP traps.

Step 4 Click the **Misc** tab.

Step 5 Check the **Show Element Manager Trace Log** check box.

Step 6 Click **OK**.

The Trace Log window opens.

Refreshing the Element Manager Display

To refresh the Element Manager display to reflect the most recent status of the server switch, do one of the following:

- From the File menu, choose **Refresh**.
- Click the **Refresh** icon ().

Launching a Telnet Session

To refresh the Element Manager display to reflect the most recent status of the server switch, do one of the following:

- From the File menu, choose **Telnet**.
- Click the **Telnet** icon ().

Closing Element Manager

To close Element Manager, from the File menu, choose **Exit**.

CHAPTER 4

Edit Tasks

These topics describe the Edit tasks for Element Manager:

Note Use the Edit menu to quickly view port and card properties. You can use the Edit menu to choose all cards or ports of the same type and then view the properties of those elements. You can perform Edit menu tasks with the Element Manager chassis display. To view and configure the server switch from the chassis display, see the "Chassis Display Tasks" section on page 2-1.

Viewing Properties of One Interface Card

To view the properties of one interface card, follow these steps:

Step 1 Click the card with properties that you want to view.

Step 2 From the Edit menu, click **Card Properties**.

A window opens and displays the properties of the card.

Step 3 Click the **Card** tab.

Table 4-1 describes the fields in this tab.

Table 4-1 Interface Card Fields

Field	Description
Admin Type (gateway cards only)	Administratively configured card type.
Card Type	Dynamically discovered card type.
Enable/Disable Card	The up and down radio buttons enable or disable the card.

Table 4-1 Interface Card Fields (continued)

Field	Description
Current Card Status	Displays up if the card can currently run traffic; otherwise, displays down.
Operational State	Displays the general condition of the interface card. The general condition may appear as any of the following: • unknown • normal • wrongBootImage • bootFailed • tooHot • booting A condition of unknown indicates an unsupported interface card. To address this condition, replace the card with a supported card. The operational state of a card must appear as **normal** for the current status of the card to appear as up. A wrong-image condition indicates that the active system image on the interface card does not match the active system image on the controller. All cards must run the same active system image as the controller card to function. A bootFailed condition indicates that the active system image on the card was incompletely or incorrectly loaded. If the other interface cards come up successfully, reset the individual card. Otherwise, reboot your entire device. The tooHot condition indicates that the card is overheating. From the Health menu, select **Status,** and then click on the **Fans** tab to see if your fans failed. The booting condition indicates that the card has not finished loading necessary image data for internal configuration.
Card Boot Stage	Boot Stage can be any of the following: • recovery • ipl • ppcboot • fpga • pic • ib • rootfs • kernel • exe • done • none

Table 4-1 Interface Card Fields (continued)

Field	Description
Card Boot Status	Boot Status can be any of the following: • upgrading • success • failed • badVersion • badCrc • memoryError • outOfSpace • programmingError • hardwareError • fileNotFound • inProgress • none
Serial Number	Factory-assigned product serial number of the card.
PCA Serial Number	Printed circuit assembly (PCA) serial number of the card.
PCA Assembly Number	Printed circuit assembly (PCA) assembly number of the card.
FRU Number	Field-replaceable unit (FRU) number of the card.
Product Version ID	Version ID of the card.
Action	Radio buttons follow these steps when you click Apply: • Take no action • Reset (reboot) the card • Delete inactive images from the card
Result	Displays the result of the last executed action from the Action field.

Viewing Properties of All Interface Cards of the Same Type

To view the properties of all interface cards of the same type, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then choose the type of card that you want to select.

Yellow selection boundaries appear around all cards of that type.

Step 2 From the Edit menu, choose **Card Properties**.

A window opens and displays a table of all of the properties of the selected cards.

Viewing Properties of One Port

This topic describes how to view properties of a single port. In addition to the properties described here, these topics let you view IP addresses and bridging properties of an Ethernet port:

- Viewing IP Addresses of an Ethernet Port, page 4-6
- Viewing Bridging Properties of an Ethernet Port, page 4-7

To view the properties of one port, follow these steps:

Step 1 Click the port with properties that you want to view.

Step 2 From the Edit menu, select **Port Properties**.

A window opens and displays the properties of the port.

- Table 4-2 describes the fields in the properties window of an Ethernet port.
- Table 4-3 describes the fields in the properties window of a Fibre Channel port.
- Table 4-4 describes the fields in the properties window of an InfiniBand port.

Table 4-2 Ethernet Port Properties Window Field Descriptions

Field	Description
Port Type	Displays the port number in slot#/port# notation.
Port Name	Port name that you can edit and apply to the port.
Enable/Disable Port	The up and down radio buttons let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation check box	Enables or disables autonegotiation on the port.
Set Port Speed	Radio buttons let you configure the speed of the port.
Current Port Speed	Displays the speed of the port.
Set Duplex	Radio buttons let you configure the duplex setting of the port.
Current Duplex	Indicates whether the port runs in full duplex mode or half duplex mode.
Enable Link Up/Down Trap	Enabled and disabled radio buttons let you configure whether or not the port sends a trap when links go up or down.
MTU	Displays the maximum transmission unit (MTU) of the port, in bytes.
MAC Address	Displays the media access control (MAC) address of the port.
Last Changed On	Time and date that a user last configured the port.
Action	Flushes the ARP table when you click Apply.
Result	Displays the result of the executed action from the Action field.

Table 4-3 Fibre Channel Port Properties Field Descriptions

Field	Description
Port Type	Port number in slot#/port# notation.
Port Name	Port name that you can edit and apply to the port.
Enable/Disable Port	Up and down radio buttons let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation	Check box that lets you enable or disable autonegotiation on the port.
Set Port Speed	Radio buttons that let you configure the speed of the port.
Current Connection Type	Type of Fibre Channel connection between the port and the SAN.
Current Port Speed	Displays the speed of the port.
Enable Link Up/Down Trap	Enabled and disabled radio buttons that let you configure whether or not the port sends a trap when links go up or down.
MTU	Maximum transmission unit (MTU) of the port, in bytes.
WWNN	World-wide node name of the HCA of the port.
WWPN	World-wide port name of the port.
FC ID	Native Fibre Channel ID of the port.
Last Changed On	Time and date of the last time that a user configured the port.

Table 4-4 InfiniBand Port Properties Field Descriptions

Field	Description
Port Type	Port number in slot#/port# notation.
Port Name	Port name that you can edit and apply to the port.
Enable/Disable Port	The up and down radio buttons that let you configure the administrative status of the port.
Current Port Status	Indicates whether or not the port is ready for use.
Physical State	Status of the physical connection to the port.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Enable Auto Negotiation	Check box that lets you enable or disable autonegotiation on the port.
Set Port Speed	Drop down menu configures the link capacity of the port in terms of its link width (1x, 4x, or 12x) and its lane speed (SDR or DDR). Valid values are 1x-SDR (2.5 Gbps), 4x-SDR (10 Gbps), 12x-SDR(30 Gbps), 1x-DDR (5 Gbps), 4x-DDR (20 Gbps), and 12x-DDR (60 Gbps).

Table 4-4 InfiniBand Port Properties Field Descriptions (continued)

Field	Description
Current Port Speed	Displays the link capacity of the port.
Power Connector Dongle Type	Displays the power connector Dongle type. This field appears only if the InfiniBand port is supporting the power connector. Possible values are as follows: • none (1) • ib4xFX (2)
Power Connector Dongle State	Indicates the power control state of dongle that is attached to a powered interface connector. Possible Values are as follows: • noStateChange(0) • on(1) • off(2)
Clear Counters	Check box allows you to clear the counters for the InfiniBand port.
Enable Link Up/Down Trap	Enabled and disabled radio buttons that let you configure whether or not the port sends a trap when links go up or down.
MTU field	Maximum transmission unit of the port, in bytes.
Last Changed On field	Time and date of the last time that a user configured the port.

Viewing IP Addresses of an Ethernet Port

To view the IP addresses of one Ethernet port, follow these steps:

Step 1 Click the Ethernet port with IP addresses you want to view.

Step 2 From the Edit menu, click **Port Properties**.

A window opens and displays the properties of the port.

Step 3 Click the **IP Addresses** tab.

The IP Addresses tab appears. Table 4-5 describes the fields in this display.

Table 4-5 IP Address Field Descriptions

Field	Description
Port	Port number, in card#port# format. A port# of 0 represents the internal gateway port of the interface card.
Address	IP address assigned to the port.
Netmask	Subnet mask assigned to the port.
BcastAddrFormat	IP broadcast address format that the port uses.
ReasmMaxSize	Size of the largest IP datagram that this port can receive and reassemble from incoming fragmented IP datagrams.

Table 4-5 IP Address Field Descriptions (continued)

Field	Description
Type	Displays primary or backup to indicate that the interface card acts as the primary or backup interface for the IP address that appears in the address field.
Status	Displays active or inactive to indicate that the card actively services IP packets addressed to the IP address in the address field or does not service packets to the specified address.

Viewing Bridging Properties of an Ethernet Port

To view the bridging properties of one Ethernet port, follow these steps:

Step 1 Click the Ethernet port with Bridging properties you want to view.

Step 2 From the Edit menu, click **Port Properties**.

A window opens and displays the properties of the port.

Step 3 Click the **Bridging** tab.

The Bridging tab appears. Table 4-6 describes the fields in this tab.

Table 4-6 Bridging Field Descriptions

Field	Description
Port	Port number, in slot#/port# format.
IEEE VLAN Tag	VLAN of the bridge group.
Bridge Group ID	Bridge group to which the port belongs. Assign the bridge group from the Ethernet menu by choosing **Bridging**.

Viewing Properties of All Ports of the Same Type

To view the properties of all ports of the same type, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then choose the type of port that you want to select.

Yellow selection boundaries appear around all ports of that type.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a table of all of the properties of the selected ports.

Configuring Interface Card Properties

You can configure interface card properties with the Edit menu or with the chassis display. For chassis display instructions, see Chapter 2, "Chassis Display Tasks". These topics describe how to configure card properties with the Edit menu:

- Configuring Administrative Card Types, page 4-8
- Enabling or Disabling a Card, page 4-9

Configuring Administrative Card Types

Configure administrative card types to reserve slots for particular interface cards. You can configure administrative card types in one of the following ways:

- Configuring One Interface Card as Administrative Card Type, page 4-8
- Configuring Multiple Cards as Administrative Card Types, page 4-8

Configuring One Interface Card as Administrative Card Type

To configure the card type for one interface card, follow these steps:

Step 1 Click the type of card you want to configure.

Step 2 From the Edit menu, choose **Card Properties**.

A window opens and displays the properties of the card.

Step 3 Click the appropriate radio button in the AdminType field, click **Apply**, and then click **Close**.

Configuring Multiple Cards as Administrative Card Types

To configure the card types for multiple interface cards, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then choose a type of card.

Yellow selection boundaries appear around all cards of that type.

Step 2 From the Edit menu, choose **Card Properties**.

A window opens and displays a table of all of the properties of the selected cards.

Step 3 In the AdminType column, click the type of the card that you want to configure.

A drop-down menu appears. Choose a value from the drop-down menu, and then repeat this step for each additional card that you want to configure.

Enabling or Disabling a Card

You can enable and disable cards using either of the following procedures:

- Enabling or Disabling Cards from a One Card Display, page 4-9
- Enabling or Disabling Multiple Cards, page 4-9

Enabling or Disabling Cards from a One Card Display

To enable or disable cards from a one-card display, follow these steps:

Step 1 Click the card that you want to enable or disable.

Step 2 From the Edit menu, choose **Card Properties**.

A window opens and displays the properties of the card.

Step 3 Click the **up** or **down** radio button, click **Apply**, and then click **Close**.

Enabling or Disabling Multiple Cards

To enable or disable cards from a multiple-card display, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then choose the type of card that you want to select.

Yellow selection boundaries appear around all cards of that type.

Step 2 From the Edit menu, choose **Card Properties**.

A window opens and displays a table of all of the properties of the selected cards.

Step 3 In the Enable/Disable Card column, click the status of the card that you want to enable or disable.

A drop-down menu appears.

Step 4 Choose **up** or **down**. Repeat this step for each additional card that you want to enable or disable.

Configuring Port Properties

You can use the Edit menu to configure port properties, or you can use the chassis display directly. To configure port properties from the chassis display, see the "Chassis Display Tasks" section on page 2-1. These topics describe how to configure port properties from the Edit menu:

- Configuring a Port Name, page 4-10
- Enabling or Disabling a Port, page 4-10
- Enabling or Disabling Autonegotiation, page 4-11
- Configuring Port Speed, page 4-12
- Clearing InfiniBand Port Counters, page 4-13

Configuring a Port Name

These tasks rename ports from a one-port display or a multiple-port display:

Configuring the Name of One Port

To configure the name of one port, follow these steps:

Step 1 Click a port with a name you want to change.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 In the Port Name field, edit the name, click **Apply**, and then click **Close**.

Configuring Multiple Port Names

To configure names for multiple ports, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports with names that you want to configure.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 Double-click the text in the Port Name column of a port that you want to rename, and then edit the name. Repeat this step for all ports that you want to rename.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling a Port

These topics describe how to enable or disable ports from a one-port display or a multiple-port display:

Enabling or Disabling One Port

To enable or disable one port, follow these steps:

Step 1 Click the port that you want to enable or disable.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 In the Enable/Disable Port field, click the **up** or **down** radio button.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling Multiple Ports

To enable or disable multiple ports, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports that you want to enable or disable.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Enable/Disable Port column, click the cell of a port that you want to enable or disable, and then choose **up** or **down** from the drop-down menu that appears.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling Autonegotiation

These topics describe how to enable or disable autonegotiation on ports from a one-port display or a multiple-port display:

- Enabling or Disabling Autonegotiation from One Port, page 4-11
- Enabling or Disabling Autonegotiation from Multiple Ports, page 4-12

Enabling or Disabling Autonegotiation from One Port

To enable or disable autonegotiation on a port from one port, follow these steps:

Step 1 Click the port for which you want to enable or disable autonegotiation.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 Check or uncheck the **Enable Auto-Negotiation** check box.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling Autonegotiation from Multiple Ports

To enable or disable autonegotiation on ports from multiple ports, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports for which you want to enable or disable autonegotiation.

Step 2 From the Edit menu, and choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Enable Auto-Negotiation column, click the cell of a port that you want to configure, and then choose **true** or **false** from the drop-down menu that appears.

Step 4 Click **Apply**, and then click **Close**.

Configuring Port Speed

These topics describe how to configure port speed from a one-port display or a multiple-port display:

- Configuring the Port Speed for One Port, page 4-12
- Configuring the Port Speed for Multiple Ports, page 4-13

Note You must disable autonegotiation on a port before you assign a speed to the port.

For an InfiniBand port connected with an SDR cable or any cable longer than 8 feet, you must manually configure the port to support SDR only.

Configuring the Port Speed for One Port

To configure port speed for one port, follow these steps:

Step 1 Click the port for which you want to configure speed.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 For an Ethernet or Fibre Channel port, in the Set Port Speed area, click the radio button that corresponds to the speed that you want to apply. For an InfiniBand port, in the Set Port Speed area. select the speed you want to apply from the drop-down menu.

Step 4 Click **Apply**, and then click **Close**.

Configuring the Port Speed for Multiple Ports

To configure the port speed on multiple ports at once, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports for which you want to configure the speed.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Set Port Speed column, click the cell of a port that you want to configure, and then choose the speed that you want to apply from the drop-down menu that appears.

Repeat this step for all ports that you want to configure.

Step 4 Click **Apply**, and then click **Close**.

Clearing InfiniBand Port Counters

These topics describe how to clear InfiniBand port counters from a one-port display or a multiple-port display:

- Clearing InfiniBand Port Counters for One Port, page 4-13
- Clearing InfiniBand Port Counters for Multiple Ports, page 4-13

See Table 7-1 on page 7-2 for descriptions of the counters reset by this procedure.

Clearing InfiniBand Port Counters for One Port

To clear InfiniBand port counters for one port, follow these steps:

Step 1 Click the port for which you want to clear the counters.

Step 2 From the Edit menu, and choose **Port Properties**.

A window opens and displays port details.

Step 3 Check the **Clear Counters** check box.

Step 4 Click **Apply**, and then click **Close**.

Clearing InfiniBand Port Counters for Multiple Ports

To clear InfiniBand port counters for multiple ports at once, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports with counters you want to clear.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Clear Counters column, click the cell of a port that you want to configure, and then choose **true** from the drop-down menu that appears.

Repeat this step for all ports that you want to configure.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling Link Up/Down Traps

These topics explain how to enable or disable link up and link down traps from a one-port display or a multiple-port display:

- Enabling or Disabling Link Up/Down Traps from One Port, page 4-14
- Enabling or Disabling Link Up/Down Traps from Multiple Ports, page 4-14

Enabling or Disabling Link Up/Down Traps from One Port

To enable or disable up/down traps for one port, follow these steps:

Step 1 Click the port that you want to configure.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 In the Enable Link Up/Down Trap field, click the **enabled** or **disabled** radio button.

Step 4 Click **Apply**, and then click **Close**.

Enabling or Disabling Link Up/Down Traps from Multiple Ports

To enable or disable link up/down traps for multiple ports, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports you want to configure.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Enable Link Up/Down Trap column, click the cell of a port that you want to configure, and then choose **enabled** or **disabled** from the drop-down menu that appears.

Repeat this step for all ports that you want to configure.

Step 4 Click **Apply**, and then click **Close**.

Executing Port Actions

Some port types can execute specific actions. These topics describe how to execute actions from a one-port display or a multiple-port display:

- Executing a Port Action for One Port, page 4-15
- Executing a Port Action for Multiple Ports, page 4-15

Executing a Port Action for One Port

To execute an action for one port, follow these steps:

Step 1 Click the port for which you want to execute and action.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays port details.

Step 3 In the Action field, click the radio button of the action that you want to execute.

Step 4 Click **Apply**, and then click **Close**.

Executing a Port Action for Multiple Ports

To execute an action for multiple ports, follow these steps:

Step 1 From the Edit menu, choose **Select All**, and then click the type of the ports for which you want to execute and action.

Step 2 From the Edit menu, choose **Port Properties**.

A window opens and displays a tabular layout of the properties of the ports.

Step 3 In the Action column, click the cell of a port on which you want to execute an action, and then choose the action from the drop-down menu that appears.

Repeat this step for every port on which you want to execute an action.

Step 4 Click **Apply**, and then click **Close**.

CHAPTER 5

Maintenance Tasks

These topics describe the Maintenance tasks of Element Manager:

Note The Maintenance menu provides opportunities to monitor your server switch and configure fundamental behavior.

Viewing Basic System Information

Basic system information includes the name and the location of your device and support resources.

To view basic system information, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens. Table 5-1 describes the fields in the window.

Table 5-1 System Info Fields

Field	Description
Description	Description of the chassis and the image that runs on the chassis.
System Uptime	Amount of time that the chassis has run since the last boot.
Last Change Made At	Date and time that a user last changed the running configuration.
Last Config Saved At	Date and time that a user last saved the running configuration as the startup configuration.
System Name	Configurable name for your server switch.
Location	Configurable location of your server switch.
Support Contact	Configurable support information for your server switch.
Rack Locator UID (select chassis)	No longer used.
SystemSyncState	Displays system synchronization state information for the Cisco SFS 7008 only.

Step 2 Click the **Backplane** tab to display the serial number, PCA serial number, PCA assembly number, FRU number, base MAC address, and chassis ID.

Step 3 Click the **Global Setting** tab to display the Global Settings.

Table 5-2 describes the fields in the Global Settings window.

Table 5-2 Global Settings Window Fields

Element	Description
Enable Ib Counter Reset	When checked, resets the Enable Ib counter.
System Operation Mode field	Choose the **Normal** radio button for non-VFrame systems and the **VFrameManaged** radio button for systems in a VFrame environment. For more information, see the VFrame documentation.

Configuring Basic System Information

Basic system information includes the name of your device, the location of your device, and support resources. These topics describe how to configure this information:

Naming Your InfiniBand Switch

To assign a hostname to your device, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the System Name field, type the name that you want to assign to the device, and then click **Apply**.

Defining Device Location

To add a physical device location description to your switch, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the Location field, type the name location of your device, and then click **Apply**.

Defining a Technical Support Resource

The technical support e-mail address that you define appears in the System frame when you refresh or restart Element Manager. To define a technical support resource, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 In the Support Contact field, type the e-mail address of your technical support provider, and then click **Apply**.

Configuring SystemOperMode

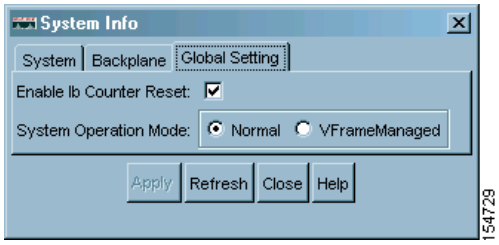
Configure SystemOperMode status to alter the behavior of the server switch to respond appropriately to a VFrame environment or a non-VFrame environment. To configure SystemOperMode, follow these steps:

Step 1 From the Maintenance menu, choose **System Info**.

The System Info window opens.

Step 2 Click the **Global Setting** tab shown in Figure 5-1.

Figure 5-1 Global Settings



Step 3 In the SystemOperMode field, click one of the following radio buttons:

- Click **Normal** to configure the server switch for a non-VFrame environment.
- Click **VFrameManaged** to configure the server switch for a VFrame-managed environment.

Step 4 Click **Apply**.

Configuring Date and Time Properties

An internal clock runs on your device, but we recommend that you configure your device to access a Network Time Protocol (NTP) server to synchronize your device with your network.

These topics describe how to configure date and time properties:

- Configuring the Date and Time, page 5-4
- Assigning NTP Servers, page 5-5

Configuring the Date and Time

To configure the date and time of the internal clock on your device, follow these steps:

Step 1 From the Maintenance menu, choose **Time**.

The Date and Time Properties window opens. The Date and Time tab appears by default.

Step 2 In the Date field, enter the date in the *MM/DD/YY* format.

Step 3 In the Time field, enter the time in *HH*:*MM*:*SS* format, and then click **Apply**.

Step 4 Click **Apply** in the Date and Time partition.

Assigning NTP Servers

To assign an NTP server to synchronize your server switch with the network, follow these steps:

Step 1 From the Maintenance menu, choose **Time**.

The Date and Time Properties window opens.

Step 2 In the NTP Server 1 field, enter the IP address of the NTP server that you want your server switch to use.

Step 3 (Optional) In the NTP Server 2 field, enter the IP address of the NTP server that you want your switch to use if your switch cannot access the primary NTP server.

Step 4 (Optional) In the NTP Server 3 field, enter the IP address of the NTP server that you want your switch to use if your switch cannot access the primary or secondary NTP servers.

Step 5 Click **Apply** in the NTP Servers partition.

Note When your device cannot access a NTP server, it defaults to the onboard clock.

Configuring the Local Time Zone and Daylight Savings Time

You can configure the time zone and daylight savings time either by selecting from a pre-configured list of time zones, or you can name and configure the details the of the time zone manually. These topics describe how to perform these tasks:

- Configuring a Time zone and Daylight Savings Time Manually, page 5-5
- Configuring a Time Zone and Daylight Savings Time from a Pre-Configured List, page 5-6

Configuring a Time zone and Daylight Savings Time Manually

To configure the time zone or daylight savings time manually, follow these steps:

Step 1 From the Maintenance menu, choose **Time ...**.

The Date and Time Properties window appears.

Step 2 Click the **Time Zone** tab.

Step 3 To configure the time zone, in the Time Zone section, enter the following information:

a. In the Name field, enter the name of a time zone.

For example, if your server switch is located in the Pacific time zone, enter **PST**. This string appears in subsequent messages that display the time.

b. In the Offset from UTC field, enter the number of hours that your time zone is offset from Coordinated Universal Time (UTC).

For Pacific Standard Time, for example, enter **- 8**.

Step 4 To configure daylight savings time, in the Daylight Saving Time section, enter the following information:

a. In the Name field, enter a name for the daylight savings time.

For example, in the Pacific time zone, enter PDT. For the period for which daylight savings time is active, this string appears in messages that display the time.

b. In the Offset from Local Time field, enter the number of hours and minutes to advance the clock while daylight savings time is active.

c. In the Start Date field, enter the date on which daylight savings time begins.

The format for the date is *mm*/*dd*/*yyyy*.

d. In the End Date field, enter the date on which daylight savings time ends.

The format for the date is *mm*/*dd*/*yyyy*.

e. In the Start Time field, enter the time of day at which daylight savings time begins.

The format for the time is *hh*:*mm* on a 24-hour clock.

f. In the End Time field, enter the time of day at which daylight savings time ends.

The format for the time is *hh*:*mm* on a 24-hour clock.

Step 5 Click **Apply**.

Configuring a Time Zone and Daylight Savings Time from a Pre-Configured List

To configure the time zone or daylight savings time from a pre-configured list, follow these steps:

Step 1 From the Maintenance menu, choose **Time ...**.

The Date and Time Properties window appears.

Step 2 Click the **Time Zone** tab.

Step 3 Click the **Select TZ** button.

The Time Zones window appears.

Step 4 From the drop-down menu, select the time zone.

Step 5 Click the **Details** button to preview the time zone information.

Step 6 Click **OK** to populate the Time Zone tab of the Data and Time window with the data for the selected time zone.

Step 7 Click **Apply**.

Configuring Basic Services

These topics describe how to configure basic services to facilitate remote access to your device:

Assigning a DNS Server

To assign a DNS server to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **DNS** tab.

Step 3 In the Server 1 field, enter the IP address of the primary DNS server that you want to use.

Step 4 (Optional) In the Server 2 field, enter the IP address of the DNS server that you want to use if your device cannot access the primary DNS server.

Step 5 In the Domain field, enter the domain to which you want your switch to belong, and then click **Apply**.

Enabling or Disabling the FTP Access

To enable or disable FTP access to and from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **FTP** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable FTP Server** check box, and then click **Apply**.

Enabling or Disabling the Telnet Access

To enable or disable Telnet access to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Telnet** tab.

Step 3 Check (to enable) or uncheck (to disable) the **Enable Telnet Server** check boxes, and then click **Apply**.

Assigning a Syslog Server

Note This task assumes that you have already configured the host and connected it to the InfiniBand fabric.

To assign a syslog server to store logs from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Syslog** tab.

Step 3 In the Remote Syslog Server One field, enter the IP address of a remote server to accept messages from your device, and then click **Apply**.

Repeat this step to add a second server to Remote Syslog Server Two.

Assigning an Authentication Method

Note SFS Server Switch product configurations with TopspinOS release 2.3.x and higher use a 128-bit MD5-based hashing scheme to store passwords.

To assign an authentication method to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Authentication** tab.

Step 3 In the Authentication Method field, click a radio button to choose a method, and then click **Apply**.

Table 5-3 describes the radio buttons that you can choose.

Table 5-3 Authentication Methods

Radio Button	Description
local	Authenticates user logins against the chassis database.
localThenRadius	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to reach any configured RADIUS server, the user is denied access.
radiusThenLocal	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user or failure to access any configured RADIUS server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
localThenTacacs	Authenticates user logins against the chassis database. Upon failure, authenticates with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, the user is denied access.
tacacsThenLocal	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user or failure to access any configured TACACS+ server, authenticates against the chassis database. If authentication against the chassis database fails, then the user is denied access.
radius	Authenticates user logins with up to three configured RADIUS servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any RADIUS server.
tacacs	Authenticates user logins with up to three configured TACACS+ servers. Upon failure to authenticate the user, the user is denied access. The authentication process checks against the chassis database only if it cannot access any TACACS+ server.

Viewing and Managing RADIUS Servers

These topics describe how to view and manage RADIUS servers:

- Viewing RADIUS Servers, page 5-10
- Adding RADIUS Servers, page 5-11
- Editing a RADIUS Server Configuration, page 5-11
- Deleting RADIUS Servers, page 5-12

Viewing RADIUS Servers

To view the RADIUS servers that you have configured your device to use to authenticate CLI and Element Manager logins, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Table 5-4 describes the fields in the Radius Servers table.

Table 5-4 Radius Server Properties Window Fields

Field	Description
Address	IP address of the RADIUS server.
Priority	Value used to configure priority of this entry. This value is not writable. The first added server gets the highest priority which is priority 1. If multiple RADIUS servers are specified the server with a higher priority is used before a server with a lower priority. No two radius servers can have the same priority.
Udp Port	Authentication port of the RADIUS server. Edit this value, and click **Apply** to configure the UDP port of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Encryption Key	Encryption key used by the radius server and client. Enter a value, and click **Apply** to configure the encryption key of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Timeout	Timeout: timeout period for any outstanding request to the server. Edit this value, and click **Apply** to configure the timeout value of the RADIUS server. The numbers to the right of the field indicate the range that this field supports.
Max Retries	Maximum number of retries that the same request can be sent to the server before the request times out. Edit this value, and click **Apply** to configure the maximum number of retries that the RADIUS server permits. The numbers to the right of the field indicate the range that this field supports.
Access Requests	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts	Number of logins to your device that the server authenticated since your device booted.
Access Rejects	Number of logins to your device that the server denied since your device booted.
Server Timeout	Number of authentications that timed out on the server since your device booted.

Adding RADIUS Servers

To add a new RADIUS server on your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click **Insert**.

The Insert Radius Server window opens.

Note Click **Close** at any time to abort this process with no changes to your device. Configurations apply only after you click **Apply**.

Step 4 In the Address field, enter the IP address of the server.

Step 5 (Optional) Edit the UDP Port field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 6 (Optional) In the Encryption Key field, enter an encryption key.

Step 7 (Optional) Edit the Timeout field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 8 (Optional) Edit the Max Retries field.

The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 Click **Insert**.

Editing a RADIUS Server Configuration

To edit a RADIUS server in your configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Identify the row of the RADIUS server that you want to reconfigure, and then double-click the cell that you want to edit.

Note You can only edit cells that have a white background.

Step 4 Edit the content of the cell.

Step 5 Click **Apply**.

Deleting RADIUS Servers

To delete a RADIUS server from your configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Radius Servers** tab.

Step 3 Click the row entry of the RADIUS server that you want to delete.

Step 4 Click **Delete**.

Viewing and Managing TACACS+ Servers

These topics describe how to view and manage TACACS+ servers:

Viewing TACACS+ Servers

To view the TACACS+ servers that you have configured your device to use to authenticate CLI and Element Manager logins, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Table 5-5 describes the fields in the TACACS+ Servers table.

Table 5-5 TACACS+ Server Properties Window Elements

Field	Description
Address	Displays the IP address of the TACACS+ server.
Priority	Value used to configure the priority of this entry. This value is not writable. The first added server gets the highest priority which is priority 1. If multiple TACACS+ servers are specified, the server with a higher priority is used before a server with a lower priority. No two TACACS+ servers can have the same priority.
Udp Port	Authentication port of the TACACS+ server. Edit this value, and click **Apply** to configure the UDP port of the TACACS+ server. The numbers to the right of the field indicate the range of integer values that this field supports.

Table 5-5 TACACS+ Server Properties Window Elements (continued)

Field	Description
Encryption Key	Encryption key used by the TACACS+ client and server. Enter a value, and click **Apply** to configure the encryption key of the TACACS+ server. The numbers to the right of the field indicate the range that this field supports.
Timeout	Timeout period for any outstanding request to the server. Edit this value, and click **Apply** to configure the timeout value of the TACACS+ server. The numbers to the right of the field indicate the range that this field supports.
Max Retries	Maximum number of retries that the same request can be sent to the server when the request times out. Edit this value, and click **Apply** to configure the maximum number of retries that the TACACS+ server permits. The numbers to the right of the field indicate the range of integer values that this field supports.
Access Requests	Number of authentication requests that the server has received from your device since your device booted.
Access Accepts	Number of logins to your device that the server authenticated since your device booted.
Access Rejects	Number of logins to your device that the server denied since your device booted.
Server Timeout	Number of authentications that timed out on the server since your device booted.

Adding a TACACS+ Server

To add a TACACS+ server to your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Click **Insert**.

Step 4 Provide an IP address for the server.

Step 5 (Optional) Change the UDP port from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 6 (Optional) Provide an encryption key.

Step 7 (Optional) Change the timeout from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 8 (Optional) Change the maximum retries from the default. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 Click **Insert**.

Editing a TACACS+ Server Configuration

To edit a TACACS+ server, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Identify the row of the server that you want to reconfigure, and then double-click the cell to edit.

Note You can only edit cells that have a white background.

Step 4 Edit the content of the cell.

Step 5 Click **Apply**.

Deleting a TACACS+ Server

To delete a TACACS+ server from your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Tacacs Servers** tab.

Step 3 Select a server.

Step 4 Click **Delete**.

Enabling HTTP Services

To configure HTTP services, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **HTTP** tab.

Step 3 Check the **Enable HTTP Server** check box.

Step 4 (Optional) Assign a port in the HTTP Port field.

Step 5 (Optional) Check the **Enable HTTP Polling** check box.

Step 6 (Optional) Check the **Enable HTTPS Server** check box.

Step 7 (Optional) Assign a port in the HTTPS Port field.

Step 8 Choose a security method from the Secure Cert Common Name field.

Step 9 Click **Apply**.

Configuring Cisco Discovery Protocol

Cisco Discovery Protocol discovers information on neighbors and status. To configure CDC services, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Discovery** tab.

Step 3 Check the **Run Discovery** check box to enable discovery.

Step 4 (Optional) Change the message interval by clicking the current value and typing a new one between 5 and 254 seconds.

Step 5 (Optional) Change the hold time by clicking the current value and typing a new one between 10 and 255 seconds.

Step 6 Click **Apply**.

Viewing the Discovery Cache

To view the discovery cache, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Services**.

The Services window opens.

Step 2 Click the **Discovery Cache** tab.

Customizing the Boot Configuration

To customize the boot configuration follow these steps:

- View the image that the switch will boot during the next reboot.
- Delete the startup configuration.
- Overwrite the startup configuration with another configuration file in your file system.

These topics describe how to perform the following tasks:

- Configuring Reboot Image, page 5-16
- Deleting or Overwriting the Startup Configuration, page 5-16

Configuring Reboot Image

To choose the image that the server switch loads when it reboots, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Boot Config**.

The Boot Configuration window opens.

Step 2 From the Image Source For Next Reboot drop-down menu, choose the image that you want the server switch to boot when it reboots.

Step 3 Click **Apply** in the Software Images partition.

Deleting or Overwriting the Startup Configuration

To delete or overwrite the startup configuration, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Boot Config**.

The Boot Configuration window opens.

Step 2 (Optional) Click the **Overwrite startup configuration with** radio button, and choose a configuration from the drop-down menu to replace the current startup configuration with another configuration file.

Note To overwrite your startup configuration with your running configuration, see the "Backing Up the Running Configuration File" section on page 5-16.

Step 3 (Optional) Click the **Delete startup configuration** radio button to configure your server switch to use the factory-default startup configuration.

Step 4 Click **Apply** in the Startup Configuration partition.

Backing Up the Running Configuration File

To back up your running configuration file, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Backup Config**.

The Backup Configuration window opens.

Step 2 Enter a filename in the Save Configuration As field.

Element Manager saves the running configuration in the configuration directory that you specify.

Note Enter **startup-config** in this field if you want to save the running configuration as the startup configuration. This process overwrites the existing startup configuration file.

Step 3 Click **Save**.

Viewing and Deleting Files in the File System

These topics describe file system tasks and concepts:

Viewing Files in the File System

To view files, such as image files, log files, and configuration files, that reside on your device, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens. Table 5-6 describes the fields in the Current Files on System table in this window.

Table 5-6 Current Files on System Table Field Descriptions

Field	Description
Slot ID	Slot of the controller card on which the file resides.
File Name	Name of the file.
File Type	Type of file. The following types may appear: • config • log • image
Size	Size of the file, in bytes.
Date	Most recent date and time that your device or a user updated the file.

Step 2 (Optional) Click **Refresh** to poll your switch and update your display to reflect the most current inventory of your file system.

Deleting Files in the File System

To delete files from your file system, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the line in the **Current Files on System** table that lists the file that you want to delete, and then click **Delete**.

A Delete File window opens.

Step 3 Click **Yes**.

Understanding Configuration Files

A configuration file is a text file that stores a list of CLI commands. These topics describe specific instances of configuration files:

- startup-config File, page 5-18
- running-config File, page 5-18

startup-config File

The main configuration file is called startup-config. This file stores all of the CLI commands necessary to completely configure a box from a factory-default state. This configuration file can be copied, backed up, and modified.

running-config File

Whenever configuration changes are made through the GUI or CLI, a CLI command is temporarily saved in a virtual configuration file called running-config. If you want to save these changes permanently, this file is copied into the startup-config file.

Any number of configuration files can be stored. For convenience and rapid configuration, files can also maintain a partial list of CLI commands. These files can also be copied into running-config for immediate use or startup-config for persistent use across reboots.

Understanding Log Files

Log files are text files that record activity, including configuration changes. Depending on their size, log files are rotated and compressed. Log files can also be exported from the system by using the **copy** command. These topics provide details about log files:

- File Management and Storage of Log Files, page 5-19
- Log Message Types, page 5-19

File Management and Storage of Log Files

The management of log files is performed automatically, but you can configure log files. Log files are stored separately from other file types, but all files share the 128 MB of flash memory. Log files are stored in syslog files.

The system checks the size of the active log file hourly, and when it exceeds 1 MB, the active log file, ts_log, is closed, compressed, and renamed ts_log.1.gz. Other ts_log.x.gz files are incremented by 1. These files can be downloaded through the Log Viewer GUI, which can create filters for troubleshooting and auditing purposes.

Log Message Types

The following levels of logging are captured:

- CONF—configuration changes; no user action is required.
- INFO—general information; no user action is required.
- WARN— abnormal condition; user intervention may be required.
- ERROR— abnormal condition; user intervention is required.
- FATAL—abnormal condition; user must reboot.
- DEBUG—occurs only after enabling tracing. See the **trace** command documentation in the *Cisco SFS Product Family Command Reference*.

Installing Software Images

Note To proceed to the software installation instructions, see the "Installing a Software Image" section on page 5-22. The sections that follow provide context and details about installing images.

The Image data that is used to configure the software is being continuously updated and enhanced. Use the latest system image data to ensure the most efficient usage of your system.

See the user's support portal at support.cisco.com for the latest upgrades.

These topics describe concepts and procedures related to installing a system image:

System Image

A system image is an unpacked and installed image file. An image file is the source from which to install a system image and it has an .img extension.

When an image file is installed, the image file is expanded into a system image. The system image is what the user will see in order to specify what the system should use to boot up each card in the system.

Image File

Image files are stored in flash memory as a single complete file with an .img extension. Each image file contains all the operating software (application software and firmware/microcode) needed by the various cards that can be installed into the system.

The system cannot use an image file directly to boot up the system. The image file must first be installed. The installation process automatically unbundles the image file and distributes the software components to each card in the system. Users do not have to be aware of individual software components. The user enters one CLI command to install an image file. See the **install** command in the *Cisco SFS Product Family Command Reference*.

The server switch operating system stores up to three images on a disk: the uninstalled image, the current system (or installed) image, and the recovery image.

The system has only enough flash memory to store:

- One system image file (active)
- One image file (inactive/uninstalled)
- One recovery image

Occasionally, you need to manually delete an image file from the InfiniBand system to make room for a new version. See the "Deleting Files in the File System" section on page 5-18.

These topics describe image concepts:

Inactive Image

An inactive image is an image that has been downloaded but has not been installed. It is not the active or system image.

The operating system can store only one inactive image. Delete inactive images through the CLI (see the "Deleting Files in the File System" section on page 5-18), or by clicking **delete** in the Element Manager.

Active Image

An active image is the current system image. An installed or active image has gone through the entire upgrade process. The system image usually has a slash (/) in its name. Do not modify or delete the installed system image.

Recovery Image

The recovery image is a default image that comes installed on the system. The recovery image can be used to quickly restore operation to the system if an image upgrade should fail.

Version Numbers

The operating system and installed system image running on the InfiniBand system determine the supported software features.

Two types of system-images are provided:

- An image for the HCA card
- An image for the Cisco SFS 7000D, Cisco SFS 7000, Cisco SFS 7008, Cisco SFS 7008P, or Cisco IB Server Switch Module.

Before configuring the InfiniBand system, check the version of the installed system image used to boot the chassis. Use this information to ensure that you upgrade to the correct software.

Copying/Downloading the Image

Upgrading the server switch operating system requires several steps, which are described in the following sections. Note that one step is to copy the image before installing it.

Table 5-7 describes several options for copying the image into the system.

Table 5-7 Copying/Downloading Image Options

Through the CLI	Through the GUI
FTP	Remote FTP Server
TFTP	Local File
SCP	Remote Secure Server

Card Status Requirements

Only cards with an oper-status of up are updated. If a card is down when you run install or a card is added after running install, follow these steps:

Step 1 Bring up the card.

Step 2 Run the installation again.

Step 3 Specify the same image file.

If the image is already installed on a card, installation skips that card.

Step 4 Be sure to specify the boot-config again so that all cards know to boot from the same system image.

Upgrading a System

The system upgrade process is summarized in the following steps:

Step 1 Set up the hardware connection for the upgrade.

Step 2 Verify the installed system image version number.

Step 3 Download an image file from a network-accessible FTP server, or download an image file remotely from a TFTP server.

Step 4 Install the new system image.

Step 5 Configure the CLI and Element Manager to use the appropriate configuration file the next time that they reboot.

Step 6 Reboot the system.

Installing a Software Image

Note Alert other users that you plan to install a new image to your server switch.

To install a software image file, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Note If you have not already imported an image file to your file system, see the "Importing Configuration Files and Image Files" section on page 5-22.

Step 2 Click the line in the Current Files on System table that lists the file that you want to install, and then click **Install**.

A verification window opens.

Note Before you install an image, verify that you have brought up all of the cards on the chassis that you want to run the new image. Cards that run a different image from the chassis cannot pass traffic.

Step 3 Click **Yes** to install the image.

Importing Configuration Files and Image Files

These topics describe how to import files to your server switch from your local host or a remote FTP server:

Importing from a Remote Server

To import files to your server switch from remote devices, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click **Import**.

The Import File window opens.

Step 3 From the File Type drop-down menu, choose the type of file to import (**image** or **configuration**).

Step 4 Click the **Remote FTP Server** radio button or the **Remote SCP Server** radio button.

Step 5 In the Server Name or IP Address field, enter the DNS name or IP address of the FTP server that holds the file that you want to import.

Step 6 In the User Name field, enter the user ID that logs you in to the FTP server.

Step 7 In the Password field, enter the password that logs you in to the FTP server.

Step 8 Enter the directory path and name of the file on the FTP server in the File Path and Name field.

Step 9 In the File Name on System field, enter the name that the file will take on your server switch.

Step 10 Click **Copy**.

Importing from Your Local Host

To import files to your server switch from your local host, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click **Import**.

The Import File window opens.

Step 3 Choose **image** or **configuration** from the File Type drop-down menu (type of file to import).

Step 4 Click the **Local File** radio button.

Step 5 Click **Choose** and navigate to the file that you want to import.

Step 6 Select the file that you want to import, and then click **OK**.

Step 7 In the File Name on System field, enter the name that the file will take on your server switch.

Step 8 Click **Copy**.

Exporting Configuration Files and Log Files

These topics describe how to export files from your server switch to your local host or a remote FTP server:

Exporting to a Remote Server

To export files from your server switch to a remote server, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the file that you want to export.

The Export button becomes active.

Step 3 Click **Export**.

The Export File window opens.

Step 4 Click either the **Remote FTP Server** or the **Remote SCP Server** radio button.

Step 5 In the Server Name or IP Address field, enter the DNS name or IP address of the FTP server that will receive the file that you export.

Step 6 In the User Name field, enter the user ID that logs you in to the FTP server.

Step 7 In the Password field, enter the password that logs you in to the FTP server.

Step 8 In the File Path and Name field, enter the path on your remote host to copy the exported file, and the name for the file.

```
/root/files/old-config.cfg
```

Step 9 Click **Copy**.

Exporting to Your Local Host

To export files from your server switch to your local host, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **File Management**.

The File Management window opens.

Step 2 Click the file that you want to export.

The Export button becomes active.

Step 3 Click **Export**.

The Export File window opens.

Step 4 Click the **Local File** radio button.

Step 5 Click **Choose**.

Step 6 Navigate to the directory where you want to copy the file, and then click **OK**.

Step 7 Click **Copy**.

Saving a Configuration File

To back up your running configuration to the standby controller on your chassis, click the **Maintenance** menu, and choose **Save Config**.

Note If you make configuration changes to the master image and then save the configuration, verify that the master and backup have synchronized, and then save the configuration on the backup as well. For more information, see the "Configuring Database Synchronization" section on page 8-11.

Rebooting the Server Switch with Element Manager

To reboot your server switch with Element Manager, follow these steps:

Step 1 Click the **Maintenance** menu, and choose **Reboot**.

Step 2 Click **OK**.

Running General Diagnostics

These topics describe how to run chassis, card, and port diagnostics:

Running Chassis Diagnostics

To run chassis diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Chassis** tab.

Step 3 In the Module Type field, click the radio button of the type of the element that you want to diagnose.

Step 4 In the Module Number field, enter the index number of the element that you want to diagnose.

Step 5 In the Test field, click the radio button of the type of test that you want to run.

Step 6 Enter the number of times that you want the test to run in the Iterations field.

Step 7 In the Action field, click the **start** radio button to begin a test or the **stop** radio button to end a test.

Step 8 In the Option field, click the error condition that you want to apply.

Step 9 Click **Apply** to execute the configuration and start or stop the test.

Running Card Diagnostics

To run card diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics** > **General**.

Step 2 Click the **Card** tab.

Step 3 Click **Insert**.

The diagnostic Insert Card window opens.

Step 4 Click the **Card** drop-down menu, and choose the card that you want to test.

Step 5 In the Test field, click the type of test that you want to execute.

Step 6 In the Iterations field, click the number of test iterations that you want to run.

Step 7 From the Action field, choose an action:

- Click the **start** radio button if you want the test to run when you click **Insert**.
- Click the **stop** radio button if you want the test to appear in the table but not execute. To run the test later, see the "Running Configured Diagnostic Tests" section on page 5-28.

Step 8 Click **Insert**.

Deleting a Card Test Entry

To delete a card test entry, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Card** tab.

Step 3 Click the row of the entry that you want to delete, and then click **Delete**.

Running Port Diagnostics

To run port diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Port** tab.

Step 3 Click **Insert**.

The Diagnostic Insert Port window opens.

Step 4 Enter a port in the Port field, or click the **...** button, choose ports, and then click **OK**.

Step 5 In the Test field, click the radio button of the test that you want to execute.

Step 6 (Optional) Check the **Data Validation** check box to validate data.

Step 7 In the Data Size field, enter the size, in bits, of the data packet that you want to send.

Step 8 In the test in the Data Pattern field, enter the data pattern that you want to iterate.

Step 9 In the Iterations field, enter the number of iterations that you want to execute.

Step 10 In the Source ID field, enter a source local ID.

Step 11 In the Target ID field, enter a destination local ID.

Step 12 From the Action field, choose an action:

- Click the **start** radio button if you want the test to execute when you click **Insert**.
- Click the **stop** radio button if you want the test to appear in the table but not execute. To execute the test later, see the "Running Configured Diagnostic Tests" section on page 5-28.

Step 13 Click **Insert**.

Deleting a Port Test Entry

To delete a port test entry, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the **Port** tab.

Step 3 Click the row of the entry that you want to delete, and then click **Delete**.

Running Configured Diagnostic Tests

To run a diagnostic test that you have already added to the Diagnostics window, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > General**.

Step 2 Click the appropriate tab for the test that you want to run.

Step 3 Identify the entry of the test that you want to run.

Step 4 Click the cell in the Action column of that entry and choose **start** from the drop-down menu.

Note The cell must display **stop** for this process to work. If the cell displays **start**, choose **stop** from the drop-down menu, and click **Apply** before performing this step.

Step 5 Click **Apply**, and then repeatedly click **Refresh** to track the progress of the test.

Viewing POST Diagnostics

These topics describe how to view power-on self-test diagnostics for cards, power supplies, and fans:

- Viewing Card POST Diagnostics, page 5-28
- Viewing Power Supply POST Diagnostics, page 5-29
- Viewing Fan POST Diagnostics, page 5-29

Viewing Card POST Diagnostics

To view card power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Card** tab.

Table 5-8 describes the fields that appear.

Table 5-8 Card POST Field Descriptions

Field	Description
Slot ID	Slot number.
POST Status	Indicates the result of the power-on-self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on self-test.

Viewing Power Supply POST Diagnostics

To view power supply power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Power Supply** tab.

Table 5-9 describes the power supply POST fields that appear.

Table 5-9 Power Supply POST Field Descriptions

Field	Description
PS ID	Power supply number.
POST Status	Indicates the result of power-on-self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on-self-test.

Viewing Fan POST Diagnostics

To view fan power-on self-test diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > POST**.

Step 2 Click the **Fan** tab.

Table 5-10 describes the fan POST fields that appear.

Table 5-10 Fan POST Field Descriptions

Field	Description
Fan ID	Fan number.
POST Status	Indicates the result of the power-on self-test: • unknown • passed • failed
PostErrorCodes	Show error(s) detected during the power-on self-test.

Viewing FRU Diagnostics

These topics describe how to view field-replaceable unit diagnostics for cards, power supplies, and fans:

- Viewing Card FRU Diagnostics, page 5-30
- Viewing Power Supply FRU Diagnostics, page 5-31
- Viewing Fan FRU Diagnostics, page 5-31

Viewing Card FRU Diagnostics

To view card field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > FRU Error**.

Step 2 Click the **Card** tab.

Table 5-11 describes the card FRU fields that appear.

Table 5-11 Card FRU Field Descriptions

Field	Description
Slot ID	Slot number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the device's vital product data.

Viewing Power Supply FRU Diagnostics

To view power supply field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > FRU Error**.

Step 2 Click the **Power Supply** tab.

Table 5-12 describes the power supply FRU fields that appear.

Table 5-12 Power Supply FRU Field Descriptions

Field	Description
PS ID	Power supply number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the vital product data of the device.

Viewing Fan FRU Diagnostics

To view fan field-replaceable unit diagnostics, follow these steps:

Step 1 Click the **Maintenance** menu, and then choose **Diagnostics > FRU Error**.

Step 2 Click the **Fan** tab.

Table 5-13 describes the fan FRU fields that appear.

Table 5-13 Fan FRU Field Descriptions

Field	Description
Fan ID	Fan number.
FruError	Shows the last hardware error (if any) detected on this field-replaceable unit. The information returned in this variable is read from the vital product data of the device.

CHAPTER 6

Health Tasks

These topics describe the Health tasks for Element Manager:

Note The Health menu provides options that let you verify the status of your server switch. With Health menu options, you can view the operational status of server switch and view logs of server switch events.

Viewing the Health Summary

To view a summary of the health of your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Summary** tab.

Table 6-1 describes the Summary tab fields.

Table 6-1 Summary Tab Field Descriptions

Field	Description
Up Time	Amount of time that the switch has been up since the last reboot.
Power	Displays a green check if all power supplies function successfully. Displays a red X if a power supply experiences a problem.
Fans	Displays a green check if all fans function successfully. Displays a red X if a fan experiences a problem.
Sensors	Displays a green check if all temperature sensors function successfully. Displays a red X if a temperature sensor experiences a problem or if the temperature exceeds the safe threshold.

Viewing Power Supply Status

To view the status of the power supplies on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Power Supplies** tab.

Table 6-2 describes the Power Supplies tab fields.

Table 6-2 Power Supplies Tab Field Descriptions

Field	Description
PS ID	Numeric identifier of the power supply. For more information about the power supplies in your device, see your hardware documentation.
Type	Type of power (AC or DC).
Admin Status	Displays the status to which a user has configured the power supply.
Oper Status	Displays up to indicate that your power supply functions and currently supplies power to your device. Displays down for faulty power supplies.
Utilization	Percentage of total power supply resources in use.
Voltage	Voltage of the power supply.
Product Serial Number	Factory-assigned product serial number.
PCA Serial Number	Printed circuit assembly (PCA) serial number.
PCA Assembly Number	Printed circuit assembly (PCA) assembly number.
FRU Number	Field-replaceable unit (FRU) number.

Viewing Fan Status

To view the status of the fans on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Fans** tab.

Table 6-3 describes the Fans tab fields.

Table 6-3 Fans Tab Field Descriptions

Field	Description
FanId	Numeric identifier of the fan. For more information about the fans in your device, see your hardware documentation.
OperStatus	Displays up if the fan functions properly; otherwise, displays down.
Speed	Speed of the fan as a percentage of maximum speed.
ProductSerialNum	Factory-assigned product serial number.
PcaSerialNum	Printed circuit assembly (PCA) serial number.
PcaAssemblyNum	Printed circuit assembly (PCA) assembly number.
FruNum	Field-replaceable unit (FRU) number.

Viewing Sensor Status

To view the status of the temperature sensors on your server switch, follow these steps:

Step 1 From the Health menu, choose **Status**.

The Health Status window opens.

Step 2 Click the **Sensors** tab.

Table 6-4 describes the Sensors tab fields.

Table 6-4 Sensors Tab Field Descriptions

Field	Description
Slot ID	Numeric identifier of the slot in which the temperature sensor resides. For more information about the slots in your device, see your hardware documentation.
Sensor ID	Numeric identifier of the temperature sensor.
Oper Status	Operational code of the sensor. The values are normal, tempAlert, currAlert, or voltAlert.
Oper Code	Temperature of the slot.
Current Temp	Current temperature of the chassis.
Alarm Temp	Chassis temperature that triggers an alarm.
Shutdown Temp	Chassis temperature that triggers a shutdown.

Viewing and Managing Server Switch Events

These topics describe how to view and manage server switch events:

Viewing Server Switch Events

When you configure your local host to receive server switch events, you can then view a log of the events. Before you view server switch events, see the "Configuring Your Host as a Trap Receiver" section on page 6-8.

To view server switch events on a host that you have configured to receive events, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens. Table 6-5 describes the fields in the window.

Step 2 (Optional) Click the **Node** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 3 (Optional) Click the **Time** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 4 (Optional) Click the **Type** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Step 5 (Optional) Click the **Description** column header to organize the Event Viewer table by node. Click the header a second time to reverse the order (from top to bottom) of the display.

Table 6-5 Event Viewer Field Descriptions

Field	Description
Node	IP address of the server switch on which the event took place.
Time	Time that the event took place.
Type	Type of event that took place.
Description	Description of the event.

Exporting Event Logs to a Text File

To export an event log, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Export**.

The Save window opens.

Step 3 Navigate to the directory on your local host on which you want to store the event log.

Step 4 In the File Name field, enter a filename for the log, and then click **Save**.

Element Manager creates a text file with the contents of the event log on your host.

Clearing Event Entries by Category

To clear event entries from the Event Viewer table, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Clear**, and then click the type of entry that you want to remove from the table.

All entries of that type disappear from the display.

Clearing All Event Entries

To clear all event entries from the Event Viewer table, follow these steps:

Step 1 From the Health menu, choose **Event Viewer**.

The Event Viewer window opens.

Step 2 Click **Clear**, and then click **All**.

All event entries disappear from the display.

Configuring Trap Receivers

These topics describe how to configure your host as a trap receiver:

Verifying Your Host as a Trap Receiver

You must configure your host to receive traps in order to view events. If no other application on your local host controls port 162, Element Manager automatically registers your local host as a trap receiver. To verify that Element Manager registered your host, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Verify that the IP address of your host appears in the Address column.

Step 3 If it appears, verify that **true** appears in the Receive Events column.

Note If your local host has multiple IP addresses (for instance, one from a LAN and one from a wireless connection), disable all IP addresses other than the LAN address, and then close Element Manager and open it again. Verify that only the LAN address appears in the Trap Receivers window. If it appears, you can enable your other addresses.

Configuring Your Host as a Trap Receiver

If you have an application (other than Element Manager) that takes over port 162 to receive and manage SNMP traps, you must add your host to the server switch configuration with Element Manager so that the application receives server switch traps. To add your host as a trap receiver, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Click **Insert**.

The Insert Trap Receivers window opens.

Step 3 In the Address field, enter the IP address of your host.

Step 4 In the Community field, enter the SNMP community of your host.

Step 5 Check the **Receive Events** check box, and then click **Insert**.

Deleting Your Host as a Trap Receiver

If you manually configured your host as a trap receiver, you must manually remove your host to de-register. To delete your host as a trap receiver, follow these steps:

Step 1 From the Health menu, choose **Trap Receivers**.

The Trap Receivers window opens.

Step 2 Click your host in the Trap Receivers table, and then click **Delete**.

Step 3 Click **Close**.

Viewing Authentication Failures and Enabling Authentication Traps

These topics describe how to view authentication failures and enable authentication traps:

- Viewing Authentication Failures, page 6-9
- Enabling Authentication Traps, page 6-10

Viewing Authentication Failures

To view authentication failures, from the Health menu, choose **Authentication**.

The Authentication window opens. Table 6-6 describes the fields in this window.

Table 6-6 Authentication Field Descriptions

Field	Description
Enable Authentication Traps	Radio buttons enable and disable authentication traps.
CLI Access Violation Count	Number of CLI access violation counts.
CLI Last Violation Time	Time of the most recent CLI access violations.
SNMP Access Violation Count	Number of SNMP access violation counts.
SNMP Last Violation Time	Time of the most recent SNMP access violations.
HTTP Access Violation Count	Number of HTTP access violation counts.
HTTP Last Violation Time	Time of the most recent HTTP access violations.

Enabling Authentication Traps

To enable authentication traps, follow these steps:

Step 1 From the Health menu, choose **Authentication**.

The Authentication window opens.

Step 2 Click the **enabled** radio button, and then click **Apply**.

Viewing and Filtering Logs

These topics describe how to view and filter logs:

- Viewing Logs, page 6-10
- Applying Filters to ts_log Displays, page 6-10

Viewing Logs

To view one of the logs in the file system on your server switch, follow these steps:

Step 1 From the Health menu, choose **Log Viewer**.

The Log Viewer window opens.

Step 2 Click **Download**.

The Download Log Files window opens.

Step 3 In the Available log files table, click the log that you want to view, and then click **Download**.

The Save As window opens.

Step 4 Navigate to the directory in which you want to save the log file, and then click **Save**.

A Download Complete window opens and displays an Open File check box.

Step 5 Check the **Open File** check box, and then click **OK**.

The log opens in the Log Viewer window.

Applying Filters to ts_log Displays

When you configure and apply filters, Element Manager removes from the display all entries that do not match the filter criteria. To filter particular entries from log displays, follow these steps:

Step 1 From the Health menu, choose **Log Viewer**.

The Log Viewer window opens.

Step 2 Open a ts_log file. For detailed instructions, see the "Viewing and Filtering Logs" section on page 6-10.

Step 3 Click **Filter**.

The Log Filter window opens.

Step 4 Select the filter attributes that you want to apply:

- All filter options are cumulative. If you choose slot 1 and WARN, the log viewer displays only logs that apply to slot 1 *and* are of the WARN type. Any WARN type messages that do not apply to slot 1 do not appear. Any slot 1 messages of other types do not appear.
- Click **Show Advanced** to reveal application options that you can add to the filter. Click an application to apply it to the filter. Press the **Ctrl** key, and click additional applications to apply multiple applications to the filter.

Step 5 Click **Apply**.

All entries that do not match the filter disappear from the display.

CHAPTER 7

Report Tasks

These topics describe the Report tasks for Element Manager:

Note Use the Report menu to view card and port statistics. With the menu, you can view all relevant statistics in a table, or you can choose statistics to create a custom graph.

Viewing Port Statistics

These topics describe how to view port statistics:

Viewing General Port Statistics

To view port statistics, follow these steps:

Step 1 In the chassis display, click the port with statistics you want to view.

Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the **Interface** tab.

A table of port statistics appears. Table 7-1 describes the fields in this table.

Table 7-1 Port Statistics Display Field Descriptions

Field	Description
InOctets	Cumulative number of octets that arrived at the port, including framing characters.
InUcastPkts	Cumulative number of incoming packets destined for a single port.
InMulticastPkts	Cumulative number of incoming packets destined for the ports of a multicast group.
InBroadcastPkts	Cumulative number of incoming packets destined for all ports on the fabric.
InDiscards	Cumulative number of inbound packets that the port discarded for a reason other than a packet error (such as the lack of buffer space).
InErrors	Number of inbound packets with errors that the port discarded.
InUnknownProtos	For packet-oriented interfaces, the number of packets received through the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received through the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always 0.
OutOctets	Total number of octets transmitted out of the interface including framing characters.
OutUcastPkts	Total number of packets that higher-level protocols requested be transmitted and which were not addressed to a multicast or broadcast address at this sublayer, including those packets that were discarded or not sent.
OutMulticastPkts	Total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sublayer, including those packets that were discarded or not sent. For a MAC layer protocol, includes both Group and Functional addresses.
OutBroadcastPkts	Total number of packets that higher-level protocols requested to be transmitted and that were addressed to a broadcast address at this sublayer, including those packets that were discarded or not sent.
OutDiscards	Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free-up buffer space.
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Configuring the Refresh Rate

Element Manager refreshes all statistics displays at regular intervals. To configure the refresh rate, follow these steps:

Step 1 In the chassis display, click the port with the refresh rate you want to change.

Step 2 From the **Report** menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the drop-down menu at the bottom of the window, and choose the interval at which you want the display to refresh.

Note You do not need to click **Apply** or **OK**. The change takes place immediately.

Viewing Fibre Channel Statistics

In addition to general statistics, the Report menu provides Fibre Channel-specific statistics for Fibre Channel gateway ports. To view Fibre Channel statistics, follow these steps:

Step 1 In the chassis display, click the Fibre Channel gateway port with statistics that you want to view.

Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the **Fibre Channel** tab.

A table of Fibre Channel statistics appears. Table 7-2 describes the fields in this table.

Table 7-2 Fibre Channel Statistics Field Descriptions

Field	Description
FcSecondsSinceLastReset	Number of seconds since the Fibre Channel port last reset.
LinkEvents	Total number of link events (such as link up, link down) processed by the Fibre Channel interface gateway(s).
FcpCmdsOutstanding	Total number of Fibre Channel protocol commands outstanding on the Fibre Channel interface gateway(s).
FcpCmdsCompleted	Total number of Fibre Channel protocol commands completed on the Fibre Channel interface gateway(s).
FcpErrors	Total number of Fibre Channel protocol errors encountered on the Fibre Channel interface gateway(s).
FcInitiatorIO	Quantity of Initiator I/O.
FcTxFrames	Number of transmitted Fibre Channel frames.
FcTxWords	Number of transmitted Fibre Channel words.
FcRxFrames	Number of received Fibre Channel frames.

Table 7-2 Fibre Channel Statistics Field Descriptions (continued)

Field	Description
FcRxWords	Number of received Fibre Channel words.
FcLIPCount	Number of Loop Initialization Primitives.
FcNOSCount	Number of not operational primitive sequences.
FcErrorFrames	Number of error frames.
FcDumpedFrames	Number of frames that the port dumped.
FcLinkFailureCount	Number of link failures.
FcLossOfSyncCount	Number of loss-of-sync errors.
FcLossOfSignalCount	Number of loss-of-signal errors.
FcPrimitiveSeqProtocolErrCount	Number of primitive sequence protocol errors.
FcInvalidTxWordCount	Number of invalid transmission word errors.
FcInvalidCRCCount	Number of invalid cyclical redundancy checks.

Viewing IP Statistics

In addition to general statistics, the Report menu provides IP-specific statistics for Ethernet gateway ports. To view IP statistics, follow these steps:

Step 1 In the chassis display, click the Ethernet gateway port with IP statistics that you want to view.

Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the **IP** tab.

A table of IP statistics appears. Table 7-3 describes the fields in this table.

Table 7-3 IP Statistics Field Descriptions

Field	Description
InReceives	Cumulative number of input datagrams (including errors) that interfaces received for the IP address that you specified with the **ip** keyword.
InHdrErrors	Cumulative number of datagrams that interfaces discarded. Reasons to discard a datagram include the following: • Bad checksums • Version number mismatches • Format errors • Exceeded time-to-live values • IP option processing errors
InHdrChksumErr	The number of input datagrams discarded due to a checksum error in their IP headers.

Table 7-3 IP Statistics Field Descriptions (continued)

Field	Description
InAddrErrors	Cumulative number of input datagrams that ports discarded because the IP address in the destination field of the header of the datagram was not a valid address to be received by the port.
ForwDatagrams	Cumulative number of datagrams that arrived at the port en-route to a final destination. For non-IP-gateway ports, this value includes only packets that the port source-routed successfully.
InUnknownProtos	Cumulative number of datagrams that the port successfully received but discarded due to an unknown or unsupported protocol.
InDiscards	Cumulative number of datagrams that the port discarded for a reason other than a problem with the datagram (such as the lack of buffer space).
InDelivers	Cumulative number of input datagrams that the port successfully delivered to IP user protocols, including the Internet Control Message Protocol (ICMP).
OutRequests	Cumulative number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in-requests. This counter does not include any datagrams counted as forw-datagrams.
OutDiscards	Cumulative number of output IP datagrams that the port discarded for a reason other than a problem with the datagram (such as the lack of buffer space).
OutNoRoutes	Cumulative number of IP datagrams that the port discarded because a route could not be found to transmit them to their destination. This counter includes any packets counted in forw-datagrams that still qualify. This counter also includes any datagrams that a server switch cannot route because all of the gateways on the server switch are down.
FragOKs	Cumulative number of IP datagrams that the port has successfully fragmented.
FragFails	Cumulative number of IP datagrams that the port discarded because the port could not fragment them. (For instance, this situation occurs when the Don't Fragment flag of the datagram is set.)
FragCreates	Cumulative number of IP datagram fragments that the port has generated.

Viewing Ethernet Statistics

In addition to general statistics, the Report menu provides IP-specific statistics for Ethernet gateway ports. To view Ethernet statistics, follow these steps:

Step 1 In the chassis display, click the Ethernet gateway port with Ethernet statistics that you want to view.

Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the **Ethernet** tab.

A table of Ethernet statistics appears. Table 7-4 describes the fields in this table.

Table 7-4 Ethernet Statistics Field Descriptions

Field	Description
SingleCollisionFrames	Count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of the out-ucast-pkts, out-multicast-pkts, or out-broadcast-pkts, and is not counted by the corresponding instance of the multiple-collision-frames object. This counter does not increment when the interface is operating in full-duplex mode.
MultipleCollisionFrames	Count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of the out-ucast-pkts, out-multicast-pkts, or out-broadcast-pkts, and is not counted by the corresponding instance of the single-collision-frames object. This counter does not increment when the interface is operating in full-duplex mode.
AlignmentErrors	Count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the Logical Link Control (LLC) or other MAC user. Received frames for which multiple obtained error conditions are counted exclusively according to the error status presented to the LLC. This counter does not increment for 8-bit wide group encoding schemes.
FCSErrors	Count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short errors. The count is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC. Coding errors detected by the physical layer for speeds above 10 Mbps will cause the frame to fail the FCS check.
SQETestErrors	Count of times that the SQE TEST ERROR message is generated by the PLS sub layer for a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function, as described in IEEE 802.3, 1998 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mbps or on interfaces operating in full-duplex mode.
DeferredTransmissions	Count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode.

Table 7-4 Ethernet Statistics Field Descriptions (continued)

Field	Description
LateCollisions	Number of times that a collision is detected on an interface later than one Ethernet slot-time unit into transmission of a packet. A late collision included in this count is also considered to be a generic collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode.
ExcessiveCollisions	Count of frames for which transmission on an interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
InternalMacTransmitErrors	Count of frames for which transmission on an interface fails due to an internal MAC sub layer transmit error. A frame is counted only if it is not counted by the corresponding instance of the late-collisions object, the excessive-collisions object, or the carrier-sense-errors object. The precise meaning of this count is implementation-specific. This object may represent a count of transmission errors on a particular interface that is not otherwise counted.
CarrierSenseErrors	Number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on an interface. This count is incremented, at most, once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode.
FrameTooLongs	Count of frames received on an interface that exceed the maximum permitted frame size. The count is incremented when the frame-too-longs status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are counted exclusively according to the error status presented to the LLC.
InternalMacReceiveErrors	Count of frames for which reception on an interface fails due to an internal MAC sub layer receive error. A frame is counted only if it is not counted by the corresponding instance of the frame-too-longs, alignment-errors, or fcs-errors object. The precise meaning of this count is implementation-specific. An instance of this object may represent a count of receive errors on a particular interface that is not otherwise counted.

Graphing Port Statistics

Element Manager provides utilities that create line charts, area charts, bar charts, and pie charts to visually represent port statistics.

To graph particular port statistics, follow these steps:

Step 1 In the chassis display, click the port with statistics that you want to view.

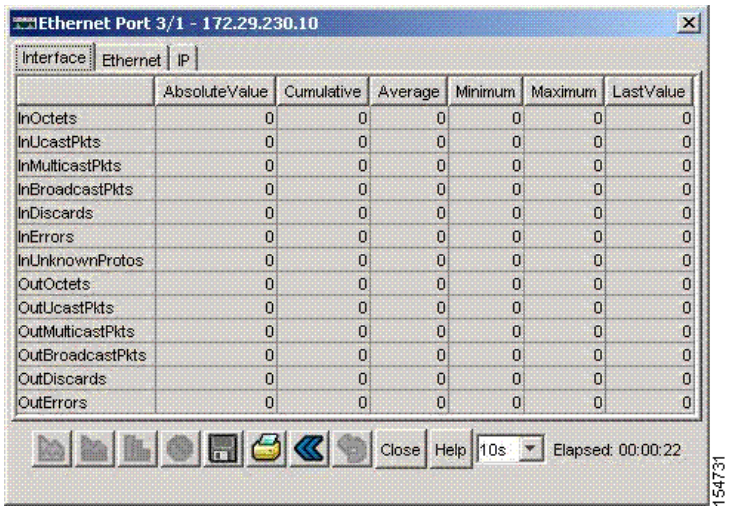
Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the **Interface** tab. (Optionally, you can click the **IP**, **Ethernet**, or **Fibre Channel** tabs, when available.)

A table of port statistics appears, as shown in Figure 7-1.

Figure 7-1 Ethernet Port Statistics



Step 4 Select the values to include in the graph using one of the following methods:

- Click-and-drag your cursor across the values that you want to graph.
- Press the **Ctrl** key, and click the values that you want to graph.

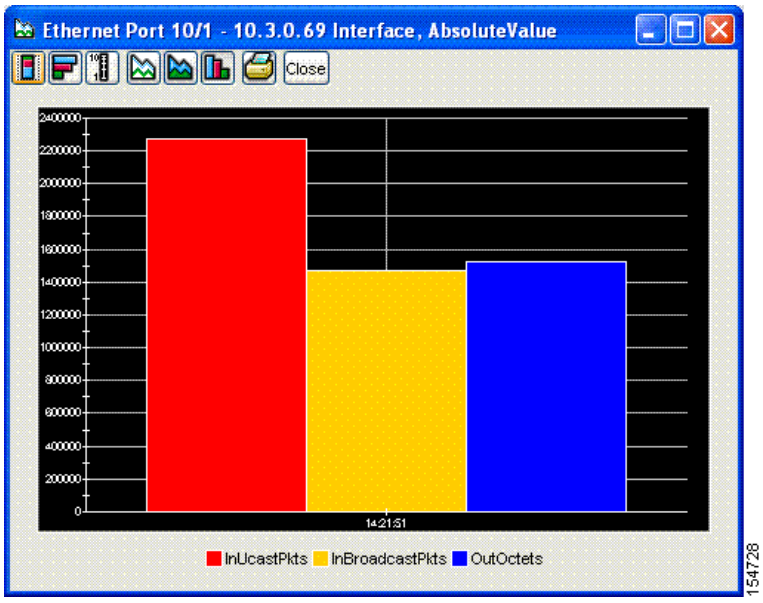
Step 5 Click the icon (see Figure 7-2) of the graph type that you want to create.

Figure 7-2 Graphing Icons

	**Line Chart**
	**Area Chart**
	**Bar Chart**
	**Pie Chart**

The graph appears. Figure 7-3 shows a bar chart example.

Figure 7-3 Bar Chart



Note With most charts, the display will reload with updated information based on the refresh rate. To configure the interval, see the "Configuring the Refresh Rate" section on page 7-3.

Using a Swap Chart Type, Layout, and Scale

With the exception of pie charts, the chart display lets you follow these steps:

- Swap between charts.
- Increase or decrease the scale of the display.
- View the chart horizontally or vertically.

Table 7-5 describes the icons used to perform these functions.

Table 7-5 Chart Icons

Icon	Function
	The Stacked icon overlays the graphical output of each statistic.
	The Horizontal icon rotates the axis of the graph by 90 degrees.
	The Log Scale icon zooms in and out.

Table 7-5 Chart Icons (continued)

Icon	Function
	The Line Chart icon displays a line chart.
	The Area Chart icon displays an area chart.
	The Bar Chart icon displays a bar chart.

Viewing Card Statistics

These topics describe how to use Element Manager to view statistics of Fibre Channel gateway cards or Ethernet gateway cards:

- Viewing Fibre Channel Card Statistics, page 7-10
- Viewing Ethernet Card Statistics, page 7-11
- Configuring the Refresh Rate, page 7-12

Viewing Fibre Channel Card Statistics

To view Fibre Channel statistics, follow these steps:

Step 1 In the chassis display, click the card with statistics you want to view.

Step 2 From the Report menu, choose **Graph Card**.

A window opens that displays the type and number of the card and presents card statistics in tabular format. Table 7-6 describes the fields in this table.

Table 7-6 Fibre Channel Card Statistics

Field	Description
LinkEvents	Total number of link events (such as the link up, link down) processed by the Fibre Channel interface gateway(s).
SrpInitiatedIos	Total number of scrip file initiated I/O requests.
SrpCmdsCompleted	Cumulative number of commands that one or all Fibre Channel gateways executed.
SrpBytesRead	Cumulative number of script file bytes read by one or all Fibre Channel gateways.
SrpBytesWritten	Cumulative number of script file bytes written by one or all Fibre Channel gateways.
SrpConnections	Total number of connections used by the script file initiator.
SrpCmdsOutstanding	Cumulative number of outstanding script file commands.
SrpErrors	Cumulative number of script file errors.

Table 7-6 Fibre Channel Card Statistics (continued)

Field	Description
FcInitiatedIos	Total number of I/O responses by the Fibre Channel device to script file initiator requests.
FcpCmdsCompleted	Cumulative number of commands that one or all Fibre Channel gateways executed.
FcpBytesRead	Cumulative number of Fibre Channel bytes read by one or all Fibre Channel gateways.
FcpBytesWritten	Cumulative number of Fibre Channel bytes written by one or all Fibre Channel gateways.
FcpCmdsOutstanding	Cumulative number of outstanding Fibre Channel commands.
FcpErrors	Cumulative number of Fibre Channel errors on one or all gateways.

Viewing Ethernet Card Statistics

To view Ethernet card statistics, follow these steps:

Step 1 In the chassis display, click the card with statistics that you want to view.

Step 2 From the Report menu, choose **Graph Card**.

A window opens that displays the type and number of the card and presents card statistics in tabular format. Table 7-7 describes the fields in this table.

Table 7-7 Ethernet Card Statistics

Field	Description
InReceives	Cumulative number of input datagrams (including errors) that interfaces received for the IP address that you specified with the **ip** keyword.
InHdrErrors	Cumulative number of datagrams that interfaces discarded. Reasons to discard a datagram include the following: • Bad checksums • Version number mismatches • Format errors • Exceeded time-to-live values • IP option processing errors
InHdrChksumErr	Cumulative number of header checksum errors.
InAddrErrors	Cumulative number of input datagrams that ports discarded because the IP address in the destination field of the header of the datagram was not a valid address to be received by the port.
ForwDatagrams	Cumulative number of datagrams that arrived at the port en-route to a final destination. For non-IP-gateway ports, this value includes only packets that the port source-routed successfully.

Table 7-7 Ethernet Card Statistics (continued)

Field	Description
InUnknownProtos	Cumulative number of datagrams that the port successfully received but discarded due to an unknown or unsupported protocol.
InDiscards	Cumulative number of datagrams that the port discarded for a reason other than a problem with the datagram (such as the lack of buffer space).
InDelivers	Cumulative number of input datagrams that the port successfully delivered to IP user protocols, including Internet Control Message Protocol (ICMP).
OutRequests	Cumulative number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in-requests. This counter does not include any datagrams counted as forw-datagrams.
OutDiscards	Cumulative number of output IP datagrams that the port discarded for a reason other than a problem with the datagram (such as the lack of buffer space).
OutNoRoutes	Cumulative number of IP datagrams that the port discarded because a route could not be found to transmit them to their destination. This counter includes any packets counted in forw-datagrams that still qualify. This counter also includes any datagrams that a server switch cannot route because all of the gateways on the server switch are down.
FragOKs	Cumulative number of IP datagrams that the port has successfully fragmented.
FragFails	Cumulative number of IP datagrams that the port discarded because the port could not fragment them. (For instance, this situation occurs when the Don't Fragment flag of the datagram is set.)
FragCreates	Cumulative number of IP datagram fragments that the port has generated.

Configuring the Refresh Rate

Element Manager refreshes all statistics displays at regular intervals. To configure the refresh rate interval, follow these steps:

Step 1 In the chassis display, click the port with the refresh rate that you want to change.

Step 2 From the Report menu, choose **Graph Card**.

A window opens that displays the type and number of the port.

Step 3 Click the drop-down menu at the bottom of the window and choose the interval at which you want the display to refresh.

Note You do not need to click **Apply** or **OK**. The change takes place immediately.

Graphing Card Statistics

Element Manager provides utilities that create line charts, area charts, bar charts, and pie charts to visually represent port statistics.

To graph particular card statistics, follow these steps:

Step 1 In the chassis display, click the card with statistics that you want to view.

Step 2 From the Report menu, choose **Graph Card**.

A window opens that displays the type and number of the port. A table of card statistics appears.

Step 3 Select the values that you want to include in the graph with one of the following methods:

- Click-and-drag your cursor across the values that you want to graph.
- Press the **Ctrl** key, and click the values that you want to graph.

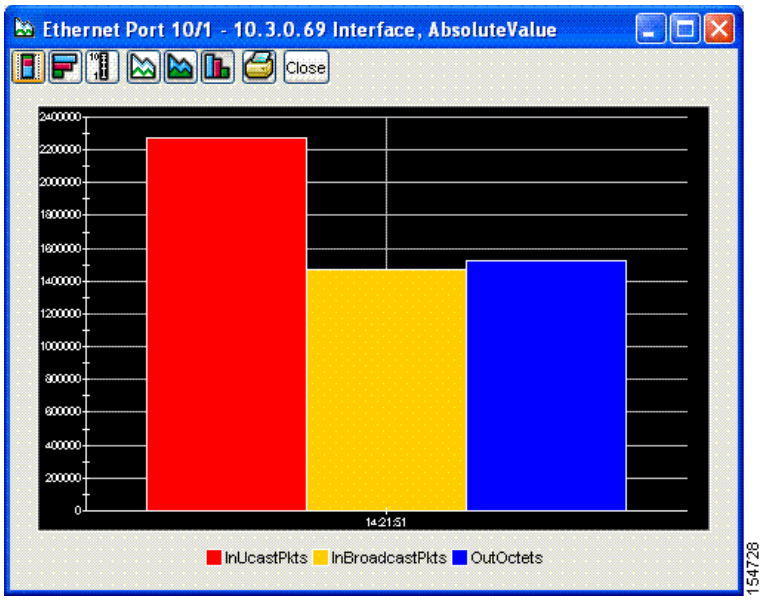
Step 4 Click the icon of the graph that you want to create. See Figure 7-4.

Figure 7-4 Graphing Icons

	**Line Chart**
	**Area Chart**
	**Bar Chart**
	**Pie Chart**

The graph appears. See Figure 7-5 for an example.

Figure 7-5 Bar Graph Example



Note With most charts, the display reloads with updated information based on the refresh rate. To configure the interval, see the "Configuring the Refresh Rate" section on page 7-12.

Using the Swap Chart Type, Layout, and Scale

With the exception of pie charts, the chart display lets you do the following:

- Swap between charts.
- Increase or decrease the scale of the display.
- View the chart horizontally or vertically.

To do these tasks, use the icons shown in Table 7-8.

Table 7-8 Charting Icons

Icon	Function
	The Stacked icon overlays the graphical output of each statistic.
	The Horizontal icon rotates the axis of the graph by ninety degrees.

Table 7-8 Charting Icons (continued)

Icon	Function
	The Log Scale icon zooms in and out.
	The Line Chart icon displays a line chart.
	The Area Chart icon displays an area chart.
	The Bar Chart icon displays a bar chart.

CHAPTER 8

InfiniBand Subnet Management Tasks

These topics describe the InfiniBand menu subnet management tasks for Element Manager:

Note See Appendix A, "InfiniBand Concepts" to familiarize yourself with the InfiniBand technology. For hardware-specific information, consult the relevant hardware documentation.

Using the InfiniBand Menu

The InfiniBand menu has two choices for performing InfiniBand subnet management tasks:

- Subnet Management
- Subnet Management (tabular format)

These topics describe how to use the Subnet Management menu option. Most of the tasks can also be performed by selecting the Subnet Management (tabular format) menu option, which presents information and configurable options in tables, but is a less user friendly way to perform your InfiniBand subnet management tasks.

Viewing and Managing Subnet Manager Properties

These topics describe procedures for performing the following tasks:

Viewing Subnet Manager Properties

To view Subnet Manager properties, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Manager window opens.

Step 2 Select a subnet.

A table of Subnet Manager properties appears under the General tab. Table 8-1 describes the fields.

Table 8-1 Subnet Management Window, General Tab Fields

Field	Description
GUID	Displays the GUID of the port on which the Subnet Manager runs.
Status	Status of the Subnet Manager. The status can be master, standby, inactive, or discovery.
Activity Count	Activity counter that increments each time that the Subnet Manager issues a subnet management packet (SMP) or that performs other management activities.
SM Key	64-bit subnet management key assigned to a Subnet Manager.
Priority	Priority of the Subnet Manager relative to other Subnet Managers in the InfiniBand network. Priority is assigned to the higher number.
Sweep Interval	Specifies how frequently a Subnet Manager queries the InfiniBand fabric for network changes.
Response Timeout	Maximum amount of time that the Subnet Manager waits for a response after it sends a packet to a port. If the Subnet Manager does not receive a response in time, the Subnet Manager identifies the port as unresponsive.
Master Poll Interval	Interval at which a slave Subnet Manager polls a master to see if it still runs.
Master Poll Retries	Number of unanswered polls that cause a slave to identify a master as dead.
Max Active SMs	Maximum number of standby Subnet Managers that a master supports. A value of 0 indicates unlimited Subnet Managers.
LID Mask Control	Number of path bits present in the base LID to each channel adapter port. Increasing the LMC value increases the number of LIDs assigned to each port to increase the number of potential paths to reach each port.
Switch Life Time	The lifetime of a packet inside a server switch. This value defaults to 20.

Table 8-1 Subnet Management Window, General Tab Fields (continued)

Field	Description
Switch Link HoQ Life	The lifetime of a packet at the head of queue of a switch port. This value defaults to 20.
CA Link HoQ Life	The lifetime of a packet at the head of queue of the host port. This value defaults to 20. **Note** This value is set automatically to the same value as Switch Link HoQ Life.
Maximum Hop Count	Specifies the number of hops. Range is from 0 to 64. Default is 64. A value of 0 causes the Subnet Manager to calculate and use the lowest possible value that will still ensure connectivity between all endpoints.
MAD Retries	Number of times that a Subnet Manager resends a MAD after not receiving a response. The default value is 5.
Node Timeout	Minimum amount of time in seconds that a HCA is unresponsive before the Subnet Manager removes it from the InfiniBand fabric. The default value is 10 seconds.
Wait Report Response	Whether or not a Subnet Manager waits to receive ReportResponse MADs in response to the Report MAD that it forwards. If this Boolean value is set to false, the Subnet Manager only sends the Report MADs once; if set to true, the Subnet Manager will continue to send the Report MADs until either the Report Response MAD is received or the maximum number of Report MADs have been sent. The default value is false.
SA MAD Queue Depth	Size of a Subnet Administrator internal queue for receiving MADs. The default value is 256.

See the "Configuring Subnet Manager Properties" procedure on page 8-4 for details on how to configure these properties.

Adding a Subnet Manager

To add a Subnet Manager to your server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 In the navigation pane, click **Subnet Managers**.

The Subnet Managers display appears in the right pane of the window.

Step 3 Click **Add**.

The Add Subnet Manager window opens.

Step 4 In the Subnet Prefix field, enter a subnet prefix.

Step 5 In the Priority field, enter a subnet priority level.

Step 6 (Optional) In the smKey field, enter a subnet management key.

Step 7 (Optional) In the LID Mask Control field, enter a value to increase the number of LIDs assigned to each port to increase the number of potential paths to reach each port.

Step 8 Click **Add**.

The new Subnet Manager appears in the Summary table in the Subnet Managers display.

Removing a Subnet Manager

To remove a Subnet Manager from your server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 In the navigation pane, click **Subnet Managers**.

The Subnet Managers display appears in the right pane of the window.

Step 3 In the Summary table in the Subnet Managers display, click the Subnet Manager that you want to remove.

Step 4 Click **Remove**.

The entry disappears from the display and the server switch configuration.

Configuring Subnet Manager Properties

The Subnet Managers navigation menu provides tuning for a number of system-wide attributes. These topics explain each attribute and describe how to configure it:

Configuring Subnet Manager Priority

Every Subnet Manager in the InfiniBand network carries a priority value, and at any given time the Subnet Manager with the highest integer value priority becomes the master Subnet Manager. To configure the Subnet Manager priority on your server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Priority field, select the value, and replace it with the value you want to apply.

The integer value 15 has the highest priority.

Step 4 Click **Apply**.

Configuring the Sweep Interval

The sweep interval specifies how frequently the Subnet Manager queries the InfiniBand fabric for network changes. To configure the sweep interval on your server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Sweep Interval field, select the value, and replace it with the value you want to apply.

This interval represents the number of seconds between sweeps.

Step 4 Click **Apply**.

Configuring Response Timeout

The response timeout of a Subnet Manager specifies the maximum amount of time that the Subnet Manager waits for a response after it sends a packet to a port. If the Subnet Manager does not receive a response in the response-time interval, the Subnet Manager identifies the port as unresponsive. To configure the response timeout, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Response Timeout field, select the value, and replace it with the value you want to apply.

The Subnet Manager measures the response timeout in milliseconds.

Step 4 Click **Apply**.

Configuring the Master Poll Interval

The master poll interval determines the interval at which the slave Subnet Manager polls the master to see if the master still runs. To configure the master poll interval, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Master Poll Interval field, select the value, and replace it with the value you want to apply.

The value represents the interval, in seconds.

Step 4 Click **Apply**.

Configuring the Number of Master Poll Retries

Master poll retries specifies the number of unanswered polls that cause a slave to identify a master as dead. To specify this value, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Master Poll Retries field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring the Maximum Supported Number of Active Standby Subnet Managers

Note To configure an unlimited number of active standby (slave) Subnet Managers, enter a value of 0. However, the limit set here is not enforced in this release.

To configure the maximum number of active standby Subnet Managers that the master Subnet Manager supports, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Max active SMs field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring LID Mask Control

Local ID mask control assigns the number of path bits present in the base LID to each channel adapter port. Increasing the LMC value increases the number of LIDs assigned to each port to increase the number of potential paths to reach each port. To configure LID mask control, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the LID Mask Control field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring Switch Lifetime

Switch lifetime is one parameter that governs the transmitter packet discard policy of switches in the subnet. It determines the lifetime of packets in a switch from the point of ingress to egress. If this parameter is set to 20 or greater, then switch lifetimes are infinite (default). See *InfiniBand Architecture Release 1.2, Volume 1* for more information.

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Switch Life Time field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring Switch Link HoQ Life

Switch link head of queue life determines how long an InfiniBand packet lives at the head of a switch port VL queue before it is discarded. If this parameter is set to 20 or greater, then HoQ lifetimes are infinite (default). See *InfiniBand Architecture Release 1.2, Volume 1* for more information.

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Switch Link HoQ Life field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring Maximum Hop Count

We recommend that InfiniBand switch elements be connected so that all paths between any pair of switch elements are the same distance (same number of hops), if possible.

The range of values is from 0 to 64. Default is 64. A value of 0 causes the Subnet Manager to calculate and use the lowest possible value that will still ensure connectivity between all endpoints.

Note Selecting any nondefault value restricts the length of paths used by the Subnet Manager. The Subnet Manager might therefore select paths that are optimal for distance, but not for other factors, such as link capacity.

To configure the maximum number of hops for an InfiniBand Subnet Manager, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Maximum Hop Count field, select the value, and replace it with the value you want to apply.

Step 4 Click **Apply**.

Configuring MAD Retries

MAD retries specifies the number of times that a Subnet Manager resends a management datagram after not receiving a response. The default value is 5.

To configure MAD retries, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the MAD Retries field, select the value, and replace it with the value that you want to apply.

Step 4 Click **Apply**.

Configuring Node Timeout

Node Timeout is the minimum amount of time in seconds that a HCA is unresponsive before the Subnet Manager removes it from the InfiniBand fabric. The default value is 10 seconds.

To configure the node timeout, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Node Timeout field, select the value, and replace it with the value that you want to apply.

Step 4 Click **Apply**.

Configuring Wait Report Response

Wait Report Response configures whether or not a Subnet Manager waits to receive ReportResponse MADs in response to the Report MAD that it forwards. If you set this Boolean value to false, the Subnet Manager only sends the Report MADs once; if you set it to true, the Subnet Manager will continue to send the Report MADs until either the Report Response MAD is received or the maximum number of Report MADs have been sent. The default value is false.

To configure the wait report response, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the Wait Report Response field, check the **Enable** box.

Step 4 Click **Apply**.

Configuring Subnet Administrator MAD Queue Depth

This procedure configures the size of a Subnet Administrator internal queue for receiving MADs. The default value is 256.

To configure the Subnet Administrator MAD queue depth, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Click the Subnet Manager that you want to configure.

A table of subnet manager properties appears under the General tab.

Step 3 In the SA MAD Queue Depth field, select the value, and replace it with the value that you want to apply.

Step 4 Click **Apply**.

Viewing and Managing Database Synchronization

Element Manager provides multiple screens that you can use to view and configure database synchronization. This section describes the following tasks:

- Viewing Database Synchronization, page 8-10.
- Configuring Database Synchronization, page 8-11.

Viewing Database Synchronization

To view database synchronization details, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Manager window opens.

Step 2 Select a subnet

Step 3 Click the **Database Sync** tab.

Details appear in the table below the tab. Table 8-2 describes the fields.

Note Database synchronization is enabled by default.

Table 8-2 Subnet Management Window, Database Sync Tab Fields

Field	Description
SM Database Synchronization	Check box to enable or disable synchronization of the database with a standby subnet manager.
Max Backup SMs	The maximum number of backup subnet managers that will synchronize with the master subnet manager.
Session Timeout	The interval, in seconds, during which a synchronization session status management datagram packet must arrive at the master subnet manager to maintain synchronization.
Poll Interval	Interval at which the master subnet manager polls an active slave subnet manager to verify synchronization.
Cold Sync Timeout	Maximum amount of time in which subnet managers can perform a cold synchronization. During the cold-sync, the master subnet manager copies all out-of-sync tables to the standby subnet manager.
Cold Sync Limit	Maximum number of cold synchronizations that can take place during the cold-sync period.
Cold Sync Limit Period	Length in seconds of the interval during which cold-syncs can occur.
New Session Delay	Amount of time in seconds that the master subnet manager waits before it attempts to initiate a synchronization session with a new subnet manager.
Resync Interval	Specifies the interval at which the master subnet manager sends a re-synchronization request to all active synchronization sessions.
State	Specifies whether or not the subnet manager is synchronized with the backup.

Configuring Database Synchronization

The database synchronization feature propagates information from the database of the master Subnet Manager to the standby Subnet Managers. These topics describe how to configure this feature:

- Enabling Subnet Manager Database Synchronization, page 8-12
- Configuring the Maximum Number of Backup Subnet Managers to Synchronize, page 8-12
- Configuring a Session Timeout, page 8-12
- Configuring the Poll Interval, page 8-13
- Configuring the Cold Synchronization Timeout Value, page 8-13
- Configuring the Cold Synchronization Limit Value, page 8-14
- Configuring the Cold Synchronization Limit Period, page 8-14
- Configuring the New Session Delay, page 8-14
- Configuring the Resynchronization Interval, page 8-15
- Viewing the Database Synchronization State, page 8-15

Enabling Subnet Manager Database Synchronization

If you are configuring more than one InfiniBand chassis in your fabric, it is likely that you will want to enable database synchronization of the Subnet Managers.

Note This feature is enabled by default.

To enable Subnet Manager database synchronization to update standby Subnet Managers with information from the master Subnet Manager, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 Click the **Database Sync** tab in the right pane.

Step 4 In the SM Database Synchronization field, check the **Enable** check box.

Step 5 Click **Apply**.

Configuring the Maximum Number of Backup Subnet Managers to Synchronize

To configure the maximum number of backup Subnet Managers that will synchronize with the master Subnet Manager, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane, click the **Database Sync** tab.

Step 4 In the Max Backup SMs field, enter an integer value.

Step 5 Click **Apply**.

Configuring a Session Timeout

To configure the session timeout interval, in seconds, during which a synchronization session status MAD packet must arrive at the master Subnet Manager to maintain synchronization, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the Session Timeout field, enter an integer value.

This value determines the timeout duration, in seconds.

Step 5 Click **Apply**.

Configuring the Poll Interval

To configure the interval, in seconds, at which the master Subnet Manager polls an active slave Subnet Manager to verify synchronization, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

Step 2 The Subnet Management window opens.

Step 3 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 4 In the right pane of the display, click the **Database Sync** tab.

Step 5 Enter an integer value in the Poll Interval field.

This value sets the poll interval, in seconds.

Step 6 Click **Apply**.

Configuring the Cold Synchronization Timeout Value

To configure the amount of time, in seconds, that a cold synchronization tries to initiate before it times out, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the **Cold Sync Timeout** field, enter an integer value.

This value sets the timeout interval, in seconds.

Step 5 Click **Apply**.

Configuring the Cold Synchronization Limit Value

To configure the maximum number of cold synchronizations to perform during a given cold synchronization period, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the Cold Sync Limit field, enter an integer value.

This value sets the maximum number of synchronizations that can occur during the synchronization period. (See "Configuring the Cold Synchronization Limit Period" section on page 8-14.)

Step 5 Click **Apply**.

Configuring the Cold Synchronization Limit Period

To specify the length of the interval during which cold synchronizations may occur, follow these steps:

Step 1 From the **InfiniBand** menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the Cold Sync Limit Period field, enter an integer value.

This value sets the length of the interval during which cold synchronizations may occur.

Step 5 Click **Apply**.

Configuring the New Session Delay

To configure the amount of time that the master Subnet Manager waits before it attempts to initiate a synchronization session with a new Subnet Manager, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the New Session Delay field, enter an integer value.

This value determines the amount of time, in seconds, that the master Subnet Manager waits before it attempts to initiate a synchronization session with a new Subnet Manager.

Step 5 Click **Apply**.

Configuring the Resynchronization Interval

To specify the interval at which the master Subnet Manager sends a resynchronization request to all active synchronization sessions, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Click the Subnet Manager that you want to configure.

Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 In the Resync Interval field, enter an integer value.

This value specifies the interval, in seconds, at which the master Subnet Manager sends a resynchronization request to all active synchronization sessions.

Step 5 Click **Apply**.

Viewing the Database Synchronization State

To view the database synchronization state and verify that the master Subnet Manager and slave Subnet Manager(s) are synchronized, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Select the Subnet Manager with the state you wan to view.

Step 3 In the right pane of the display, click the **Database Sync** tab.

Step 4 Look at the **State** field.

Viewing and Managing Nodes and Ports

This section provides procedures for performing the following tasks:

Viewing Node Information

To view Subnet Manager node information, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Expand the Subnet Manager that you want to view.

Step 3 Select **Nodes**.

The Nodes in Subnet tab displays the Node GUID, Type, Description, Number of Ports, System Image GUID, and the Vendor ID information. See Table 8-3 for details.

Step 4 Click **Show Advanced** to display the additional information about each of the nodes in the subnet. This information includes Base Version, Class Version, Port GUID, Partition Cap, Device ID, Revision, and Local Port Number. Table 8-3 describes these fields.

Table 8-3 Nodes in Subnet Tab Fields

Field	Description
Node GUID	GUID of the node.
Type	Type of node being managed. The value appears as channel adapter, switch, router, or error. An error entry indicates an unknown type.
Description	Text string describing the device.
Number of Ports	Number of physical ports on the node.
System Image GUID	GUID of an associated supervisory node. No supervisory node exists if the output displays 00:00:00:00:00:00:00:00.
Vendor ID	Device vendor ID. The value appears the same for all ports on the node.
Base Version	Supported base management datagram (MAD) version. Indicates that this channel adapter, switch, or router supports versions up to and including this version. See section 13.4.2, “Management Datagram Format,” in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
Class Version	Supported MAD class format version. Indicates that this channel adapter, switch, or router supports versions up to, and including, this version.
Device ID	Manufacturer-assigned device identification.
Revision	Manufacturer-assigned device revision.
Partition Cap	Capacity of entries in the partition table for channel adapter, router, and the switch management port. The value appears the same for all ports on the node. This defaults to at least 1 for all nodes including switches. You cannot configure this value.
Local Port Number	The link port number from which this subnet management packet (SMP) arrived. The value appears the same for all ports on the node.

Viewing Port Information

To view information about specific ports, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Expand the Subnet Manager with ports you want to view.

Step 3 Select **Nodes**.

Step 4 Expand **Nodes.**

Step 5 Expand the computer icon for the node with ports you want to view

Step 6 Select a specific port to see the information described in Table 8-4. Figure 8-1 shows a sample display.

Figure 8-1 Individual Port Information

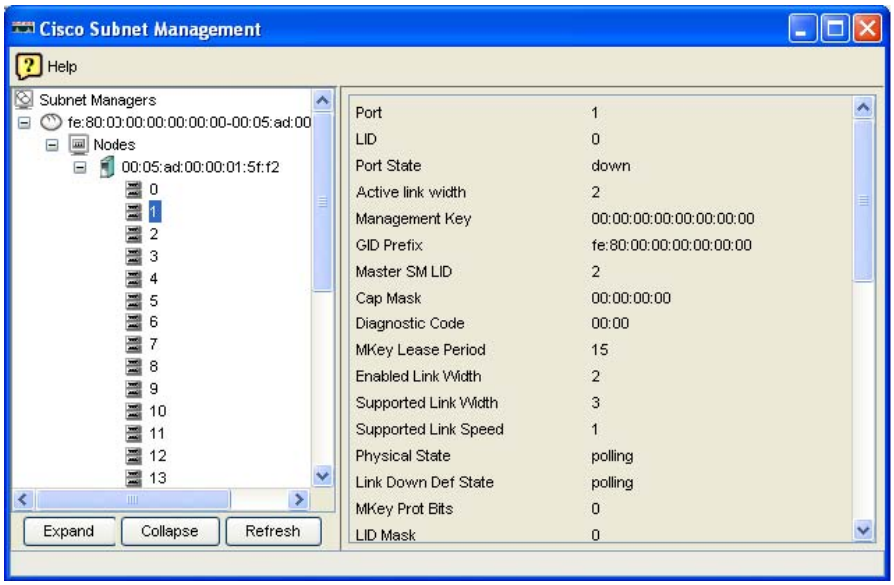


Table 8-4 Ports Field Descriptions

Field	Description
Port	Local port number for this port.
LID	16-bit base LID of this port.
Port State	State of the port, as follows: • noStateChange • sleep • polling • disabled • portConfigurationTraining • linkup • linkErrorRecovery • reserved • active • down
Active link width	Used in conjunction with Active Link Speed to determine the link rate between two nodes. The value appears as 1x, 4x, or 12x.
Management Key	64-bit management key for this port. See section 14.2.4, "Management Key" and 3.5.3, "Keys," in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
GID Prefix	64-bit Global identifier prefix for this port. The subnet manager assigns this prefix based upon the port routes and the rules for local identifiers. See section 4.1.3, "Local Identifiers," in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
Master SM LID	16-bit base LID of the master subnet manager managing this port.
Cap Mask	The capability mask identifies the functions that the host supports. 32-bit bitmask that specifies the supported capabilities of the port. A bit value of 1 (one) indicates a supported capability. The bits are 0, 11-15, 18, 21-31 (Reserved and always 0.), 1 IsSM, 2 IsNoticeSupported, 3 IsTrapSupported, 4 IsResetSupported, 5 IsAutomaticMigrationSupported, 6 IsSLMappingSupported, 7 IsMKeyNVRAM (supports M_Key in NVRAM), 8 IsPKeyNVRAM (supports P_Key in NVRAM), 9 Is LED Info Supported, 10 IsSMdisabled, 16 IsConnectionManagementSupported, 17 IsSNMPTunnelingSupported, 19 IsDeviceManagementSupported, 20 IsVendorClassSupported.Values are expressed in hexadecimal.
Diagnostic Code	16-bit diagnostic code. See section 14.2.5.6.1 "Interpretation of Diagcode," in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information. This field does not currently apply to your server switch.
MKey Lease Period	Initial value of the lease-period timer, in seconds. The lease period is the length of time that the M_Key protection bits are to remain non-zero after a SubnSet (PortInfo) fails an M_Key check. After the lease period expires, clearing the M_Key protection bits allows any subnet manager to read (and then set) the M_Key. Set this field to 0 to indicate that the lease period never expires. See *InfiniBand Architecture®, Vol. 1, Release 1.1*, section 14.2.4, "Management Key."

Table 8-4 Ports Field Descriptions (continued)

Field	Description
Enabled Link Width	Enabled link width (bandwidth). The value can be one of the following: • no state change • 1x • 4x • 1x, 4x • 8x • 1x, 8x • 4x, 8x • 1x, 4x, 8x • 12x • 1x, 12x • 4x, 12x • 1x, 4x, 12x • 8x, 12x • 1x, 8x, 12x • 4x, 8x, 12x • 1x, 4x, 8x, 12x • reserved • linkwidthsupported value
Supported Link Width	Supported link width. The value appears as one of the following: • 1x, • 1x, 4x • 1x, 4x, 8x • 1x, 4x, 12x, • 1x, 4x, 8x, 12x • reserved
Supported Link Speed	Supported link speed. The value appears as one of the following: • sdr • sdr, ddr
Physical State	Indicates the physical state of the port, whether or not electricity flows between nodes and that they can perform a handshake. The value appears as noStateChange, sleeping, polling, disabled, portConfigurationTraining, linkup, or linkErrorRecovery. The state, upon power-up, defaults to polling.
Link Down Def State	Default LinkDown state to return to. The value appears as noStateChange, sleeping, or polling. See section 5.5.2, “Status Outputs (MAD GET),” *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
MKey Prot Bits	Management key protection bits for the port. The bits are 0, 1, 2, and 3. See section 14.2.4.1, “Levels of Protection,” *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.

Table 8-4 Ports Field Descriptions (continued)

Field	Description
LID Mask	Local-identifier mask control (LMC) for multi-path support. A LMC resides on each channel adapter and router port on the subnet. It provides multiple virtual ports within a single physical port. The value of the LMC specifies the number of path bits in the LID. A value of 0 (zero) indicates one LID can apply to this port. See sections 3.5.10, "Addressing," and 4.1.3, "Local Identifiers," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
Active Link Speed	Speed of an active link. The value appears as one of the following: • sdr • ddr
Enabled Link Speed	Maximum speed that the link can handle. The value appears as one of the following: • sdr • ddr • sdr, ddr
Neighbor MTU	Active maximum transmission unit enabled on this port for transmit. Check the MTU cap value at both ends of every link and use the lesser speed. The value appears as 256, 512, 1024, 2048, or 4096.
MasterSmSL	Administrative service level required for this port to send a non-SMP message to the subnet manager.
Virtual Lanes Cap	Maximum range of data virtual lanes supported by this port. The value appears as vl0, vl0-Vl1, vl0-Vl3, vl0-Vl7, or vl0-Vl14. See also oper-VL. Each port can support up to 15 virtual lanes (VLs 0 - 15). The VL-cap field displays the range of those lanes (for example, lanes 0 - 7) that the port currently supports.
Virtual Lane High Limit	Maximum high-priority limit on the number of bytes allowed for transmitting high-priority packets when both ends of a link operate with multiple data virtual-lanes. Used with the virtual-lane arbitration table. The maximum high-limit matches the VLArbHighCap on the other side of the link and then negotiating downward.
VLArbHighCap	Highest arbitration value allowed by the arbiter in determining the next packet in a set of packets to send across the link. Used with the virtual-lane arbitration table and specified as a VL/Weight pair. See section 14.2.5.9, "VL Arbitration Table," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
VLArb Low Cap	Lowest arbitration value allowed by the arbiter in determining the next packet in a set of packets to send across the link. Used with the virtual-lane arbitration table and specified as a VL/Weight pair. See section 14.2.5.9, "VL Arbitration Table," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
MTU Cap	Used in conjunction with Neighbor MTU to determine the maximum transmission size supported on this port. The lesser of MTU cap and Neighbor MTU determines the actual MTU used. The value appears as 256, 512, 1024, 2048, or 4096.
VL Stall Count	Number of sequentially dropped packets at which the port enters a VLStalled state. The virtual lane exits the VLStalled state (8 * HLL) units after entering it. See section 18.2.5.4, "Transmitter Queuing," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for a description of HLL.

Table 8-4 Ports Field Descriptions (continued)

Field	Description
HOQ Life	Maximum duration allowed to packets at the head of a virtual-lane queue. Used with VL Stall Count to determine the outgoing packets to discard.
Oper VL	Administrative limit for the number of virtual lanes allowed to the link. Do not set this above the Virtual Lanes Cap value. The value appears as vl0, vl0-Vl1, vl0-Vl3, vl0-Vl7, or vl0-Vl14.
In Partition Enforcement	Boolean value that indicates whether or not to support optional partition enforcement for the packets that were received by this port. No default value applies.
Out Partition Enforcement	Boolean value that indicates whether or not to support optional partition enforcement for the packets transmitted by this port. No default value applies.
In Filter RawPacket Enforcement	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets that were received by this port. No default value applies.
Out Filter RawPacket Enforcement	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets transmitted by this port. No default value applies.
MKeyViolation	Number of subnet management packets (SMPs) that have been received on this port with invalid M_Keys since initial power up or the last reset. See section 14.2.4, "Management Key," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
PKeyViolation	Number of subnet management packets that have been received on this port with invalid P_Keys since initial power up or the last reset. See section 9.2.7, "Partition Key (P_KEY)," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
QKeyViolation	Number of subnet management packets that have been received on this port with invalid Q_Keys since initial power up or the last reset. See section 10.2.4, "Q Keys," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
GUID Cap	Number of GUID entries allowed for this port in the port table. Any entries that exceed this value are ignored on write and read back as zero. See section 14.2.5.5, "GUIDCap," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
Subnet Timeout	Maximum propagation delay allowed for this port to reach any other port in the subnet. This value also affects the maximum rate at with traps can be sent from this port. Switch configuration affects delay. Requestors can use this parameter to determine the interval to wait for a response to a request. Duration matches (4.096 ms * 2^SubnetTimeout).
Response Time	Maximum time allowed between the port reception of a subnet management packet and the transmission of the associated response. See section 13.4.6.2, "Timers and Timeouts," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.

Table 8-4 Ports Field Descriptions (continued)

Field	Description
Local Phys Error	Threshold at which ICRC, VCRC, FCCRC, and all physical errors result in an entry into the BAD PACKET or BAD PACKET DISCARD states of the local packet receiver. See section 7.12.2, "Error Recovery Procedures," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
Local Overrun Error	Threshold at which the count of buffer overruns, across consecutive flow-control update periods, results in an overrun error. A possible cause of such errors is when an earlier packet has physical errors and the buffers are not immediately reclaimed.

Routing Around Nodes and Ports

These topics describe how to route around nodes and ports using the Nodes displays:

- Routing Around Nodes, page 8-22
- Routing Around Ports, page 8-23

For a complete discussion of routing around components, including routing around chassis, see the "Routing Around Components in an InfiniBand Network" section on page 8-33.

Routing Around Nodes

To route around a node or to re-include a node that had previously been excluded, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Expand the Subnet Manager that manages the node you want to work on.

Step 3 Expand **Nodes.**

A list of nodes managed by the subnet manager appears in the left pane.

Step 4 Select the node you want to exclude from routing calculations or include in routing calculations.

Step 5 Right-click on the highlighted node.

Step 6 Select **Start Routing Around** or **Stop Routing Around**.

Routing Around Ports

To route around a port, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens. Each Subnet Manager appears in the navigation pane with a Subnet Manager icon ( ).

Step 2 Expand the Subnet Manager that you want to view.

Step 3 Expand **Nodes.**

A list of nodes managed by the subnet manager appears in the left pane.

Step 4 Expand the node containing the port you want to work on.

Step 5 Select the port you want to exclude from routing calculations or to include in routing calculations.

Step 6 Right-click on the highlighted port.

Step 7 Select **Start Routing Around** or **Stop Routing Around**.

Viewing and Managing Partitions

This section provides procedures for performing the following tasks:

- Viewing Partitions, page 8-23
- Creating a Partition, page 8-24
- Removing a Partition, page 8-24
- Enabling or Disabling IPoIB for a Partition, page 8-25
- Viewing Partition Details, page 8-25
- Adding Full Members to a Partition, page 8-25
- Adding Limited Members to a Partition, page 8-26

Viewing Partitions

To view the partitions on your InfiniBand network, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with partitions that you want to view.

The navigation menu expands.

Step 3 Click the **Partitions** ( ) branch.

The partitions summary appears in the right pane. Table 8-5 describes the fields in this pane.

Table 8-5 Partitions Summary Field Descriptions

Field	Description
Partition Key	Partition key (numeric identifier) of the partition.
Full Member Count	Number of full partition members.
Limited Member Count	Number of limited partition members.
IPoIB	Specifies whether IPoIB is enabled for this partition.

Creating a Partition

To create an InfiniBand partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager under which you want to create a partition.

Step 3 Select the **Partitions** ( ) branch.

Step 4 Click **Add**.

The Add Partition window opens.

Step 5 In the PKey field, enter a partition key for the new partition.

Step 6 Check the **IPoIB** check box to enable or uncheck to disable IPoIB for the partition.

Step 7 Click **OK**.

Removing a Partition

To delete a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with partition that you want to delete.

Step 3 Expand the **Partitions** ( ) branch.

Step 4 Click the partition in the Summary display that you want to remove, and then click **Remove**.

Enabling or Disabling IPoIB for a Partition

Disabling IPoIB removes all current multicast group members and prevents further multicast joins. To enable or disable IPoIB on a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the partitions for which you want to enable or disable IPoIB.

The navigation menu expands.

Step 3 Click the **Partitions** ( ) branch.

The partitions summary appears in the right pane.

Step 4 Click on the summary line of the partition for which you want to enable or disable IPoIB.

Step 5 Click **Edit**.

The Add Partition window opens.

Step 6 Check the **IPoIB** check box to check (enable) or uncheck (disable) IPoIB for the partition.

Step 7 Click **OK**.

Viewing Partition Details

To view partition details, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with partitions that you want to view.

Step 3 Expand the **Partitions** ( ) branch to display all partitions.

Step 4 Click the partition key of the partition with details that you want to view.

The members (full and limited) of the partition appear in the display.

Note To view the GUIDs of the Server Switch management ports in the display, click **Show Switch Mgmt Ports**. Click **Hide Switch Mgmt Ports** to remove these GUIDs from the display.

Adding Full Members to a Partition

Full members of a partition can communicate to other full members and to limited members.

These topics describe how to add full members to a partition:

- Adding Available Members to a Partition, page 8-26
- Adding Unavailable Members to a Partition, page 8-26

Adding Available Members to a Partition

To add available members to a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the partition to which you want to add a member.

Step 3 Expand the **Partitions** ( ) branch to display all partitions in the navigation menu.

Step 4 Select the partition key of the partition to which you want to add members.

The members (full and limited) of the partition appear in the display.

Step 5 In the Available Members field, click the port that you want to add to the partition, and then click the right arrow next to the Full Members field.

Adding Unavailable Members to a Partition

To add unavailable members (members that do not appear in the Available Members pool) to a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the partitions to which you want to add a member.

Step 3 Expand the Partitions ( ) branch to display all partitions in the navigation menu.

Step 4 Click the partition key of the partition to which you want to add members.

The members (full and limited) of the partition appear in the display.

Step 5 Click **Add Other**.

The Add Other Partition Member window opens.

Step 6 In the Node GUID field, enter the GUID of the host that includes the port(s) that you want to add to the partition.

Step 7 In the Port field, specify the port(s) that you want to add to the partition.

Step 8 Click the **Full** radio button, and then click **Add**.

Adding Limited Members to a Partition

Limited members of a partition can communicate with full members of the partition but not with other limited members.

These topics describe how to add limited members to a partition:

- Adding Available Limited Members, page 8-27
- Adding Unavailable Members, page 8-27

Adding Available Limited Members

To add available limited members to a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the partition to which you want to add a member.

The navigation menu expands.

Step 3 Expand the **Partitions** ( ) branch to display all partitions in the navigation menu.

Step 4 Click the partition key of the partition to which you want to add members.

The members (full and limited) of the partition appear in the display.

Step 5 In the Available Members field, click the port that you want to add to the partition, and then click the right arrow next to the Limited Members field.

Adding Unavailable Members

To add an unavailable member (member does not appear in the Available Members pool) to a partition, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the partition to which you want to add a member.

Step 3 Expand the **Partitions** ( ) branch to display all partitions in the navigation menu.

Step 4 Select the partition key of the partition to which you want to add members.

The members (full and limited) of the partition appear in the display.

Step 5 Click **Add Other**.

The Add Other Partition Member window opens.

Step 6 In the Node GUID field, enter the GUID of the node that includes the port(s) that you want to add to the partition.

Step 7 In the Port field, specify the port(s) that you want to add to the partition.

Step 8 Click the **Limited** radio button, and then click **Add**.

Viewing and Managing Multicast Groups

This section provides procedures for performing the following tasks:

Viewing Multicast Groups

To view the multicast groups on your InfiniBand network, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with partitions that you want to view.

The navigation menu expands.

Step 3 Select the **Multicast Groups** ( ) branch.

The multicast groups summary appears in the right pane. Table 8-6 describes the fields in this pane.

Table 8-6 Multicast Group Summary Field Descriptions

Field	Description
MGID	Numeric multicast group identifier of each multicast group on the InfiniBand fabric.
QKey	16-bit Q-Key of this multicast group.
MTU	Maximum transmission unit of the multicast group.
PKey	Partition key of the multicast group.

Viewing Multicast Group Details

To view multicast group details, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with multicast groups that you want to view.

The navigation menu expands.

Step 3 Expand the **Multicast Groups** ( ) branch to display all groups in the navigation menu.

Step 4 Click the MGID of the multicast group with details that you want to view, and then click the **General** tab.

Multicast group details appear in the display. Table 8-7 describes the fields in this display.

Table 8-7 Multicast Group General Details Field Descriptions

Field	Description
QKey	16-bit Q-Key of this multicast group.
MLID	16-bit LID of this multicast group
MTU	Maximum transmission unit of the multicast group.
TClass	Traffic class for the multicast group.
PKey	16-bit Partition Key for this multicast group.
Rate	Traffic rate of this multicast group.
Packet Life Time	Maximum estimated time for a packet to traverse a path within the multicast group.
SL	Service level of this multicast group.
Flow Label	Flow label used for this multicast group.
Hop Limit	Identifies the maximum number of hops a packet can take before being discarded.
Scope	Scope of this multicast group.
User Configured	Displays true if a user configured the entry; otherwise displays false.

Viewing Multicast Group Members

To view multicast group members, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with multicast groups that you want to view.

The navigation menu expands.

Step 3 Expand the **Multicast Groups** ( ) branch to display all groups in the navigation menu.

Step 4 Click the MGID of the multicast group with details that you want to view.

Multicast group members appear in a table at the bottom of the display. Table 8-8 describes the fields in this display.

Table 8-8 Multicast Group Members Field Descriptions

Field	Description
Port GID	Global identifier of a port that belongs to the multicast group.
Join State	Displays whether the port is a full member or limited member of the group.
Proxy Join Status	This field displays false except for trusted requests. For details, see *InfiniBand Architecture®, Vol. 1, Release 1.1*.

Configuring Multicast Groups

To configure multicast groups, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Manager window opens.

Step 2 Expand a subnet.

Step 3 Select **Multicast Groups**.

Step 4 Click **Add**.

Step 5 From the drop-down list, select **MGID**.

Step 6 In the Multicast Group ID field, enter an MGID.

Step 7 (Optional) In the QKey field, enter a queue key.

Step 8 In the MTU field, select a value to configure the maximum transmission unit of the group.

Step 9 In the PKey field, enter a partition key.

Step 10 In the Rate field, select a rate.

Step 11 In the Service Level field, enter an integer value (between 0 and 15).

Step 12 Click **Add**.

Note The TClass, Packet Lifetime, Flow Label, and Hop Limit attributes are not supported in this release.

Configuring IPoIB Broadcast Multicast Groups

To configure IPoIB broadcast multicast groups, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Manager window opens.

Step 2 Expand a subnet.

Step 3 Select **Multicast Groups**.

Step 4 Click **Add**.

Step 5 From the drop-down list, choose **IPoIB**.

Step 6 (Optional) In the QKey field, enter a queue key.

Step 7 From the drop-down list, select an MTU value.

Step 8 Enter a partition key in the PKey field.

Step 9 From the Rate field, select a data rate.

Step 10 In the Service Level field, enter an integer value (between 0 and 15).

Step 11 In the Scope field, choose a scope value.

Step 12 Click **Add**.

Note The TClass, Packet Lifetime, Flow Label, and Hop Limit attributes are not included in this release.

Viewing InfiniBand Services

To view the InfiniBand services that run on your server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with services that you want to view.

Step 3 Click the **Services** ( ) branch.

Details of InfiniBand services appear in the right pane. Table 8-9 describes the fields in the Summary section of the pane.

Table 8-9 Services Summary Field Descriptions Pane

Field	Description
Name	ASCII identifier of the service.
Service Id	Numeric identifier that nodes use to call the service.
Service GID	64-bit ID of the service.
PKey	16-bit multicast GID address.

Table 8-10 describes the fields in the Services Details section of the display.

Table 8-10 Services Details Field Descriptions

Field	Description
Service Name	ASCII identifier of the service.
Service Id	Numeric identifier that nodes use to call the service.
Service GID	GID of the node that provides the service.
Service PKey	16-bit P-Key.
Lease	Lease period remaining (in seconds) for this service. A value of 4294967295 means that the lease is indefinite.
Key	128-bit service key.
Data (8 bit)	Header of the data type 8.
Data (16 bit)	Header of the data type 16.
Data (32 bit)	Header of the data type 32.
Data (64 bit)	Header of the data type 64.

Viewing and Managing InfiniBand Routes

This section provides procedures for performing the following tasks:

- Viewing InfiniBand Routes, page 8-32
- Routing Around Components in an InfiniBand Network, page 8-33
- Removing Routes from the Route-Around Table, page 8-35

Viewing InfiniBand Routes

To view the route between a pair of LIDs in the InfiniBand fabric, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with services that you want to view.

Step 3 Select the **Routes** ( ) branch.

Step 4 Select the **Route Filter** tab

InfiniBand routes fields appear in the right pane.

Step 5 In the Source LID field, enter the source LID of the route.

Step 6 In the Destination LID field, enter the destination lid of the route.

Step 7 Click **Show Route**.

Step 8 Click the **Switch Route** tab.

Table 8-11 describes the fields under the Switch Route tab.

Table 8-11 Switch Route Field Descriptions

Field	Description
Node GUID	Global unique ID of the node.
In Port	Port of ingress.
Out Port	Port of egress.

Step 9 Click the **Switch Element Route** tab.

Table 8-12 describes the fields under the Switch Element Route tab.

Table 8-12 Switch Element Route Field Descriptions

Field	Description
Chassis GUID	Global unique ID of the node.
In Port	Port of ingress.
Out Port	Port of egress.

Routing Around Components in an InfiniBand Network

To route around a chassis, nodes, or ports that are accumulating errors or to route around a component that you want to remove, follow the steps outlines in the subsections that follow.

Uses of this feature include the following:

- Isolating ports that have accumulated errors to avoid a potential job failure. The route-around feature enables you to stop traffic from passing over a link while a job is still running, without disrupting the job.
- Isolating a specific component, such as an InfiniBand switch card, allowing that component to be removed without the potential for job failure. You might do this, for example, before component upgrade or other replacement.

Caution The route-around feature has the potential to exclude any chassis, node, or port from routing calculations to the extent that it is possible to disable entirely a connection between a pair of endpoints. Use care to avoid segmenting the InfiniBand fabric when using this feature.

Note You can also route around nodes or ports (but not chassis) from the Nodes table as described in the "Routing Around Nodes and Ports" section on page 8-22.

These topics describe how to route around components in an InfiniBand network:

Viewing Route-Around Information

To view active route-around operations, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with services that you want to view.

Step 3 Select the **Routes** () branch.

Step 4 Select the **Route Around** tab.

Excluded routes appear in the right pane. Table 8-13 describes the fields in the pane.

Table 8-13 Route Around Tab Field Descriptions Pane

Field	Description
Type	Type of component excluded. Possible values are port, node, and chassis.
GUID	GUID of the excluded node, chassis, or node of the excluded port.
Port Number	Excluded port number.

Adding Routes to the Route-Around Table

To add a component to the route-around table, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the routing information you want to change.

Step 3 Select the **Routes** () branch.

Step 4 Select the **Route Around** tab.

Step 5 Click **Add**.

A Route Around dialog box appears.

Step 6 In the Add Route Around dialogue box, define the route you want to exclude from routing calculations:

a. In the Type drop-down menu, select the **Port**, **Node**, or **Chassis** to be excluded.

b. In the GUID field, enter the GUID of the node or chassis.

c. In the Port Number field, specify the port number if you selected Port from the Type drop-down menu.

Step 7 Click **Add**.

Removing Routes from the Route-Around Table

To remove a route-around from the table, follow these steps.

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with the routing information you want to change.

Step 3 Select the **Routes** () branch.

Step 4 Select the **Route-Around** tab.

Step 5 Select the route-around that you want to remove from the table.

Step 6 Click **Remove**.

Viewing Other Subnet Managers Information

To view information on other Subnet Managers in the network, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with neighbor subnets managers that you want to view.

The navigation menu expands.

Step 3 Expand **Subnet Managers Info**.

The Port GUID, Priority, and Subnet Manager state information appears in the right pane.

Table 8-14 describes the fields in the Details pane.

Table 8-14 Subnet Managers Information Details Pane

Field	Description
Port GUID	Displays the port GUID of the networking device on which the Subnet Manager runs.
SM Key	64-bit subnet management key assigned to the Subnet Manager. The Subnet Manager key serves as the prefix of all GIDs and brands nodes as members of this subnet.

Table 8-14 Subnet Managers Information Details Pane (continued)

Field	Description
Activity Count	Activity counter that increments each time the Subnet Manager issues a subnet management packet (SMP) or that performs other management activities.
Priority	Priority of the Subnet Manager relative to other Subnet Managers in the network. The number 15 has the highest priority.
SM State	State of the Subnet Manager.

Note This menu provides information on subnet managers that are not local to the chassis to which an Element Manager is connected.

Viewing Event Subscriptions

To view the Subnet Management event subscriptions information, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

The Subnet Management window opens.

Step 2 Expand the Subnet Manager with event subscriptions that you want to view.

The navigation menu expands.

Step 3 Choose **Event Subscriptions**.

The LID, Node GUID, and Port Number information appears in the right pane.

Table 8-15 describes the fields under Subnet Management Event Subscriptions Details.

Table 8-15 Subnet Management Event Subscriptions Details Pane

Field	Description
LID	Local ID of the subscriber.
Node GUID	Global unique ID of the subscriber node.
Port Number	Port number of the subscriber.
Source QPN	24-bit source queue pair number of the subscriber.
GID	Global ID.
LID Range Start	Lowest legal Local ID number.
LID Range End	Highest legal Local ID number.
Is Generic	If ‘true,” forward all generic traps. If “false,” forward all vendor-specific traps.
Type	Type of trap for which you subscribed.
Trap Number Device ID	If generic, this is the trap number for which you subscribed. If not generic, this is the device ID for which you subscribed. 0xFFFF means forward all trap numbers/device IDs.

Table 8-15 Subnet Management Event Subscriptions Details Pane (continued)

Field	Description
Response Time Value	Response Time Value of the subscriber.
Producer Type Vendor ID	If not generic, this is the 24-bit IEEE OUI assigned to the vendor.

Viewing Forwarding Tables

This section provides procedures for performing the following tasks:

- Viewing Multicast Forwarding Information, page 8-37
- Viewing Linear Forwarding Information, page 8-37

Viewing Multicast Forwarding Information

To view the multicast forwarding configuration, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

Step 2 Click the **MulticastForwardings** tab.

Table 8-16 describes the information that appears.

Table 8-16 Multicast Forwarding Entries

Field	Description
Node Guid	GUID of the switch node in the subnet with the FDB that you want to access.
MLID	Local ID of the multicast group.
Port Mask 0	Shows to which ports a multicast packet for the given LID will be transmitted.
Port Mask 1	Port mask.

Viewing Linear Forwarding Information

To view the linear forwarding configuration, follow these steps:

Step 1 From the InfiniBand menu, choose **Subnet Management**.

Step 2 Click the **LinearForwardings** tab.

Table 8-17 describes the displayed fields.

Table 8-17 Linear Forwarding Entries

Field	Description
Node Guid	GUID of the switch node in the subnet with the FDB that you want to access.
LID	Local ID.
Port Number	Port number of the port through which the given LID will be forwarded.

CHAPTER 9

InfiniBand Performance Management Tasks

These topics describe the InfiniBand menu tasks for Element Manager that relate to performance management:

Note See Appendix A, "InfiniBand Concepts" to familiarize yourself with the InfiniBand technology. For hardware-specific information, consult the relevant hardware documentation.

Using the InfiniBand Menu

The InfiniBand menu has two choices for performing InfiniBand performance management tasks:

- Performance Management
- Performance Management (tabular format)

This section describes how to use the Performance Management menu option. Most of the tasks can also be performed by choosing the Performance Management (tabular format) menu option, which presents information and configurable options in tables, but is a less user-friendly way to perform your InfiniBand performance management tasks.

Enabling and Disabling InfiniBand Port Performance Management

Use performance management to view InfiniBand port counters, test connectivity between InfiniBand ports, and monitor InfiniBand ports for errors.

These topics describe how to enable and disable InfiniBand port performance management:

Enabling Performance Management

To enable InfiniBand-port performance management, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Click the subnet of the ports that you want to manage (for instance, fe:80:00:00:00:00:00:00).

The Port Counter Configuration display appears in the right pane of the window.

Step 3 Click the **Enable** radio button.

Disabling Performance Management

To disable performance management, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Click the subnet of the ports that you want to manage (for instance, fe:80:00:00:00:00:00:00).

The Port Counter Configuration display appears in the right pane of the window.

Step 3 Click the **Disable** radio button.

Enabling and Managing Port Monitoring

These topics describe how to enable and manage port monitoring:

Enabling Port Monitoring

To enable port monitoring, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Select the **Port Monitor** branch.

Step 4 Click the **General** tab.

Step 5 From the State drop-down menu, choose **Enable**.

Note **Enable** enables port monitoring only for the ports that are configured in the Monitor Port Config table; **enableAll** enables port monitoring for all ports regardless of whether the port is configured in the Monitor Port Config table or not.

Step 6 Click **Apply**.

Configuring Port Monitoring

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

The navigation tree expands.

Step 3 Select the **Port Monitor** branch.

Step 4 Click the **General** tab.

Step 5 In the Polling Period field, enter an integer value between 1 and 600 to configure the number of seconds between polls.

Step 6 In the Start Delay field, enter an integer value between 1 and 600 to configure the delay between startup and polling.

Configuring Port Monitoring Thresholds

To configure port monitoring thresholds, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

The navigation tree expands.

Step 3 Select the **Port Monitor** branch.

Step 4 Click the **Threshold** tab.

Step 5 Enter an integer value in the fields where you want to apply a threshold. Enter **none** in the fields to which you do not want to apply a threshold.

Step 6 Click **Apply**.

Viewing Port Monitoring Errors

To view port monitoring errors, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

The navigation tree expands.

Step 3 Select the **Port Monitor** branch.

Step 4 Click the **Port Errors** tab.

Step 5 Port errors are displayed.

Resetting Counters

You can reset counters for the following:

- Resetting Counters on a Hop, page 9-4
- Resetting Counters on All Ports on a Node, page 9-5
- Resetting Counters on All Ports in a Connection, page 9-5
- Resetting All Counters in a Subnet, page 9-5

Resetting Counters on a Hop

To reset counters on a hop, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Expand the connection that includes the hop that you want to clear.

Step 5 Right-click the hop with counters you want to clear, and choose **Clear counters on this Hop**.

Resetting Counters on All Ports on a Node

To reset counters on all ports of a node, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Expand the connection that includes the node that you want to clear.

Step 5 Right-click the node with counters you want to clear, and choose **Clear counters on this Node**.

Resetting Counters on All Ports in a Connection

To reset counters on all ports in a connection, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Right-click the connection with counters you want to clear, and choose **Clear counters on this Connection**.

Resetting All Counters in a Subnet

To reset all counters in a subnet, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Right-click the **Connection Counters** branch, and choose **Clear Counters for All Connections**.

Monitoring Connections

To monitor connections, you complete tasks such as:

Creating a Connection to Monitor

To create a connection to monitor, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Choose **Connection Counters**.

The Monitored Connection tab appears in the right pane of the window.

Step 4 Click **Add**.

The Add Connection window opens.

Step 5 In the Source LID field, enter a source LID.

Note To view available source and destination LIDs, return to the main Element Manager display, click the **InfiniBand** menu, choose **Subnet Management**, and then click the **SwitchRoute** tab. For more information, see the "Viewing and Managing InfiniBand Routes" section on page 8-32.

Step 6 In the Destination LID field, enter a destination LID.

Step 7 Check the **Enable Connection Monitoring** check box.

Note If this check box is not selected, you can view only counter information and cannot view monitoring information.

Step 8 Click **Add**.

The connection entry appears under the Monitored Connections tab.

Viewing Monitored Connections

These instructions assume that you have already defined connections to monitor. To view monitored connections, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

The navigation tree expands.

Step 3 Select the **Connection Counters** branch.

The Monitored Connection tab appears in the right pane of the window. Table 9-1 describes the fields in this pane.

Table 9-1 Monitored Connections Field Descriptions Pane

Field	Description
Subnet Prefix	Subnet prefix of the monitored connection.
Source LID	16-bit source Local ID of the connection.
Destination LID	16-bit destination Local ID of the connection.
Error Status	Displays unknown, exceeded, or notExceeded to indicate if the error value has exceeded the threshold that you configured. To configure thresholds, see the "Configuring Port Monitoring Thresholds" section on page 9-3.
Util Status	Displays unknown, exceeded, or notExceeded to indicate if the utilization value has exceeded the threshold that you configured. To configure thresholds, see the "Configuring Port Monitoring Thresholds" section on page 9-3.

Viewing Connection Counters

Each hop in the display is a port on a node. When connections move through nodes, they enter the node in one hop (GUID A, port a), and exit in another hop (GUID A, port b). Though the GUIDs of subsequent hops may match, the ports do not match. To view connection counters, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The **Performance Management** window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Select the connection with counters that you want to view.

Step 5 Click the **Connection Counters** tab.

Table 9-2 describes the fields in the display.

Table 9-2 Connection Counters Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the subnet on which each hop resides.
Node Guid	Global unique ID of the node (switch chip, HCA, or TCA) of the next-hop port.
Port Number	Port number (on the appropriate node) of the hop.
Chassis Guid	Global Unique ID (GUID) of the chassis.
Slot Number	Slot of the port.
Ext Port Number	External port number of the port.
Data Is Valid	Displays true or false.
Symbol Errors	Number of symbol errors on the port.
Link Recovery Errors	Number of link recovery errors on the port.
Link Downs	Number of link-down errors on the port.
Received Errors	Number of received errors that the port experienced.
Received Remote Physical Errors	Number of physical errors that the port experienced.
Received Switch Relay Errors	Number of switch relay errors that the port experienced.
Transmitted Discards	Number of transmitted discards that occurred on the port.
Transmitted Constraint Errors	Number of Transmitted Constraint errors that the port experienced.
Received Constraint Errors	Number of Received Constraint errors that the port experienced.
Local Link Integrity Errors	Number of logical link integrity errors on the port.
Excessive Buffer Overrun Errors	Number of excessive buffer overrun errors on the port.
VL15 Dropped	Number of VL15 drops on the port.
Transmitted Data	Volume of transmitted data on the port.
Received Data	Volume of received data on the port.
Transmitted Packets	Volume of transmitted packets on the port.
Received Packets	Volume of received packets on the port.

Viewing Connection Monitor Counters

To view connection monitor counters, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Select the connection with counters that you want to view.

Step 5 Click the **Connection Monitor Counters** tab.

Table 9-3 describes the fields in the tab.

Table 9-3 Connection Monitor Counters Field Descriptions

Field	Description
Node Guid	Global unique ID of the InfiniBand node of the hop port.
Port Number	Port number of the hop.
Chassis Guid	GUID of the chassis that includes the connection.
Slot Number	Slot number of the port(s) in the connection.
Ext Port Number	External port number of the connection port.
Error Type	Type of error that occurred.

Testing Connections

To test connections, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Select the connection with counters that you want to view.

Step 5 Click the **Test Connection** tab.

Step 6 Click **Test**.

Viewing Port Counters of Connections

To view port counters, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Connection Counters** branch.

Step 4 Expand the connection with port counters that you want to view.

Step 5 Select the port (in GUID - port-number format) with counters that you want to view.

Table 9-4 describes the fields in this display.

Table 9-4 Port Counters Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the subnet on which each hop resides.
Node Guid	Global unique ID of the node (switch chip, HCA, or TCA) of the next-hop port.
Port Number	Port number (on the appropriate node) of the hop.
Chassis Guid	GUID of the chassis that includes the connection.
Slot Number	Slot number of the port(s) in the connection.
Ext Port Number	External port number of the connection port.
Symbol Errors	Total number of symbol errors detected on one or more lanes.
Link Recovery Errors	Total number of times the port training state machine has successfully completed the link error recovery process.
Link Downs	Total number of times that the port training state machine has failed the link error recovery process and downed the link.
Received Errors	Total number of packets containing an error that was received on the port. These errors are as follows: • Local physical errors (ICRC, VCRC, FCCRC, and all physical errors that cause entry into the bad state) • Malformed data packet errors (Lver, length, VL) • Malformed link packet errors (operand, length, VL) • Packets discarded due to buffer overrun
Received Remote Physical Errors	Total number of packets marked with the EBP delimiter received on the port.
Received Switch Relay Errors	Total number of packets received on the port that were discarded because they could be forwarded by the switch relay. Reasons for this are as follows: • DLID mapping. • VL mapping. • Looping (output port = input port).
Transmitted Discards	Total number of outbound packets discarded by the port because the port is down or congested. Reasons for this are as follows: • Output port is in the inactive state. • Packet length has exceeded neighbor MTU. • Switch lifetime limit has been exceeded. • Switch HOQ limit has been exceeded.

Table 9-4 Port Counters Field Descriptions (continued)

Field	Description
Transmitted Constraint Errors	Total number of packets not transmitted from the port for the following reasons: • FilterRawOutbound is true and packet is raw. • PatitionEnforcementOutbound is true and packet fails the partition key check, the IP version check, or the transport header version check.
Received Constraint Errors	Total number of packets received on the port that are discarded for the following reasons: • FilterRawInbound is true, and packet is raw. • PartitionEnforcementInbound is true and the packet fails the partition key check, the IP version check, or the transport header version check.
Local Link Integrity Errors	Number of times that the frequency of packets containing local physical errors exceeded local_phy_errors.
Excessive Buffer Overrun Errors	Number of times that overrun errors' consecutive flow control update periods occurred with at least one overrun error in each period.
VL15 Dropped	Number of incoming VL15 packets dropped due to resource limitations on port selected by PortSelect.
Transmitted Data	(Optional) Shall be zero if not implemented. Total number of data octets, divided by 4, transmitted on all VLs from the port selected by PortSelect. This includes all octets between (and not including) the start of packet delimiter and VCRC. It excludes all link packets. You may choose to count data octets in groups larger than four but are encouraged to choose the smallest group possible. Results are still reported as a multiple of four octets.
Received Data	(Optional) Shall be zero if not implemented. Total number of data octets, divided by 4, received on all VLs from the port selected by PortSelect. This includes all octets between (and not including) the start of packet delimiter and VCRC. It excludes all link packets. You may choose to count data octets in groups larger than four but are encouraged to choose the smallest group possible. Results are still reported as a multiple of four octets.
Transmitted Packets	(Optional) Shall be zero if not implemented. Total number of data packets, excluding link packets, transmitted on all VLs from the port selected by PortSelect.
Received Packets	(Optional) Shall be zero if not implemented. Total number of data packets, excluding link packets, received on all VLs from the port selected by PortSelect.

Viewing InfiniBand Port Counters

These topics describe how to view InfiniBand port counters:

Viewing Port Counters

To view port counters, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Port Counters** branch.

Step 4 View port counters using one of the following methods:

- Click the GUID with port counters that you want to view; all available port counters appear.
- Expand the GUID of the node with port counters that you want to view, and then select the port with counters that you want to view.

Counters appear for that individual port. Table 9-5 describes the fields in the port counters display.

Table 9-5 Port Counters Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the subnet on which each hop resides.
Node Guid	Global unique ID of the node (switch chip, HCA, or TCA) of the next-hop port.
Port Number	Port number (on the appropriate node) of the hop.
Chassis Guid	GUID of the chassis that includes the connection.
Slot Number	Slot number of the port(s) in the connection.
Ext Port Number	External port number of the connection port.
Symbol Errors	Total number of symbol errors detected on one or more lanes.
Link Recovery Errors	Total number of times the port training state machine has successfully completed the link error recovery process.
Link Downs	Total number of times the port training state machine has failed the link error recovery process and downed the link.

Table 9-5 Port Counters Field Descriptions (continued)

Field	Description
Received Errors	Total number of packets containing an error that were received on the port. These errors are as follows: • Local physical errors (ICRC, VCRC, FCCRC, and all physical errors that cause entry into the "bad" state) • Malformed data packet errors (Lver, length, VL) • Malformed link packet errors (operand, length, VL) • Packets discarded due to buffer overrun
Received Remote Physical Errors	Total number of packets marked with the EBP delimiter received on the port.
Received Switch Relay Errors	Total number of packets received on the port that were discarded because they could be forwarded by the switch relay. Reasons for this are as follows: • DLID mapping. • VL mapping. • Looping (output port = input port).
Transmitted Discards	Total number of outbound packets discarded by the port because the port is down or congested. Reasons for this are as follows: • Output port is in the inactive state. • Packet length has exceeded neighbor MTU. • Switch lifetime limit has been exceeded. • Switch HOQ limit has been exceeded.
Transmitted Constraint Errors	Total number of packets not transmitted from the port for the following reasons: • FilterRawOutbound is true, and packet is raw. • PatitionEnforcementOutbound is true and the packet fails the partition key check, the IP version check, or the transport header version check.
Received Constraint Errors	Total number of packets received on the port that are discarded for the following reasons: • FilterRawInbound is true, and packet is raw. • PartitionEnforcementInbound is true and packet fails partition key check, IP version check, or transport header version check.
Logical Link Integrity Errors	Number of times that the frequency of packets containing local physical errors exceeded local_phy_errors.
Excessive Buffer Overrun Errors	Number of times that overrun errors consecutive flow control update periods occurred with at least one overrun error in each period.
VL15 Dropped	Number of incoming VL15 packets dropped due to resource limitations on port selected by PortSelect.

Table 9-5 Port Counters Field Descriptions (continued)

Field	Description
Transmitted Data	(Optional) Value is zero if not implemented. Total number of data octets, divided by 4, transmitted on all VLs from the port selected by PortSelect. This includes all octets between (and not including) the start of the packet delimiter and the VCRC. It excludes all link packets. You may choose to count data octets in groups larger than four but are encouraged to choose the smallest group possible. Results are still reported as a multiple of four octets.
Received Data	(Optional) Shall be zero if not implemented. Total number of data octets, divided by 4, received on all VLs from the port selected by PortSelect. This includes all octets between (and not including) the start of the packet delimiter and the VCRC. It excludes all link packets. You may choose to count data octets in groups larger than four but are encouraged to choose the smallest group possible. Results are still reported as a multiple of four octets.
Transmitted Packets	(Optional) Shall be zero if not implemented. Total number of data packets, excluding link packets, transmitted on all VLs from the port selected by PortSelect.
Received Packets	(Optional) Shall be zero if not implemented. Total number of data packets, excluding link packets, received on all VLs from the port selected by PortSelect.

Enabling or Disabling Monitoring a Port

To enable or disable port monitoring for a specific port, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Port Counters** branch.

Step 4 Expand the GUID of the node with port counters that you want enable or disable.

Step 5 Right click the port for which you want to enable or disable monitoring.

Step 6 From the drop-down menu, select **Enable Port Monitoring** or **Disable Port Monitoring**.

Viewing Cumulative Port Counters

To view cumulative port counters, follow these steps:

Step 1 From the InfiniBand menu, choose **Performance Management**.

The Performance Management window opens.

Step 2 Expand the subnet of the connections that you want to monitor.

Step 3 Expand the **Port Counters** branch.

Step 4 Expand the node of the port with cumulative counters that you want to view.

Step 5 Click the port with navigation counters that you want to view.

Step 6 Click the **Port Cumulative Counters** tab.

Table 9-6 describes the fields in the tab.

Table 9-6 Cumulative Port Counters Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the subnet on which each hop resides.
Node Guid	Global unique ID of the node (switch chip, HCA, or TCA) of the next-hop port.
Port Number	Port number (on the appropriate node) of the hop.
Chassis Guid	Global Unique ID (GUID) of the chassis.
Slot Number	Slot of the port.
Ext Port Number	External port number of the port.
Error Status	Displays true or false.
Util Status	Number of symbol errors on the port.
Symbol Errors	Number of link recovery errors on the port.
Link Recovery Errors	Number of link-down errors on the port.
Link Downs	Number of received errors that the port experienced.
Received Errors	Number of physical errors that the port experienced.
Received Remote Physical Errors	Number of switch relay errors that the port experienced.
Received Switch Relay Errors	Number of transmitted discards that occurred on the port.
Transmit Discards	Number of Transmit Constraint errors that the port experienced.
Transmit Constraint Errors	Number of Received Constraint errors that the port experienced.
Received Constraint Errors	Number of logical link integrity errors on the port.
Logical Link Integrity Errors	Number of excessive buffer overrun errors on the port.
Excessive Buffer Overrun Errors	Number of VL15 drops on the port.
VL15 Dropped	Volume of transmitted data on the port.
Transmit Data	Volume of received data on the port.
Received Data	Volume of transmitted packets on the port.
Transmit Packets	Volume of received packets on the port.

Table 9-6 Cumulative Port Counters Field Descriptions (continued)

Field	Description
Received Packets	Subnet prefix of the subnet on which each hop resides.
Transmit Rate	Global unique ID of the node (switch chip, HCA, or TCA) of the next-hop port.
Received Rate	Port number (on the appropriate node) of the hop.

CHAPTER 10

InfiniBand Topology View Tasks

These topics describe the InfiniBand menu tasks that can be performed through the Element Manager Topology view:

Note This section provides information to familiarize you with the InfiniBand technology. For hardware-specific information, consult the relevant hardware documentation.

Launching the Topology View

This topic describes launching the topology view. To view specific server switch components or TCS, see Viewing Internal Server Switch Components and TCAs, page 10-3.

To launch the topology view, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

Note Navigation icons appear at the top of the InfiniBand Topology window. Table 10-1 describes these icons.

Table 10-1 InfiniBand Topology Navigation Icons

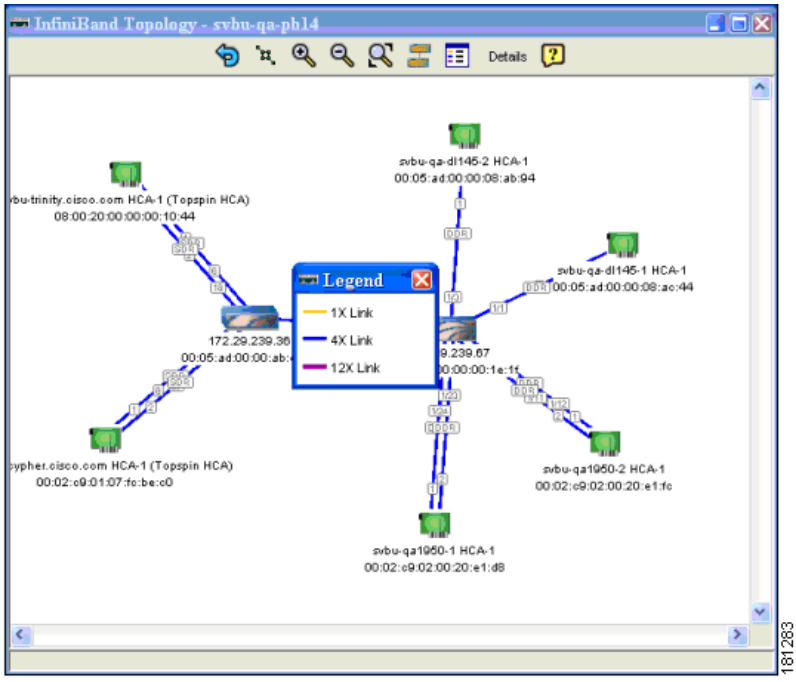
Icon'	Description
	The Refresh icon refreshes the topology display.
	The Layout icon evenly arranges the switch and HCA icons.

Table 10-1 InfiniBand Topology Navigation Icons (continued)

Icon'	Description
	The Zoom In icon enlarges the display.
	The Zoom Out icon condenses the display.
	The Fit to Screen icon zooms in or out to fit the topology in the window.
	The Specify Cisco Devices icon opens the Specify Cisco Devices dialog box to add Server Switches to the display.
	The Legend icon displays the different colors that represent different types of links.
Details	The Subnet Details icon displays subnet details. For more information, see the "Viewing Subnet Details" section on page 10-4.
	The Help icon launches the online help.

Figure 10-1 shows a sample topology view.

Figure 10-1 Topology View



Viewing Internal Server Switch Components and TCAs

To view the internal server switch components and target channel adapters (TCAs) inside a server switch, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Note Navigation icons appear at the top of the InfiniBand Topology window. Table 10-2 describes these icons.

Table 10-2 Internal InfiniBand Topology Navigation Icons

Icon	Description
	The Layout icon evenly arranges the switch and HCA icons.
	The Zoom In icon enlarges the display.
	The Zoom Out icon condenses the display.
	The Fit to Screen icon zooms in or out to fit the topology in the window.
	The Layout icon evenly arranges the switch and HCA icons.
SMAs	The Subnet Management Agents icon displays Subnet Manager agent details. For information, see the "Viewing Subnet Management Agents" section on page 10-11.
	The Help icon launches the online help.

Viewing Subnet Details

These topics describe how to view subnet details:

Viewing Nodes

To view the nodes in the topology view, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) In the Enabled column, check the check box of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Click **Details**.

The InfiniBand Subnet Details window opens.

Step 5 Click the **Nodes** tab.

Table 10-3 describes the fields in this tab.

Table 10-3 Nodes Tab Field Descriptions

Field	Description
SubnetPrefix	Subnet prefix of the node.
GUID	Global unique ID (GUID) of the node.
Description	Optional text string describing this node.
Type	Type of node being managed.
NumPorts	Number of physical ports on this node.
SystemImageGUID	System image GUID of this node. All nodes within a particular system (chassis) are assigned the same system image GUID.

Viewing Ports

To view the ports in the topology view, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) In the Enabled column, check the check box of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Click **Details**.

The InfiniBand Subnet Details window opens.

Step 5 Click the **Ports** tab.

Table 10-4 describes the fields in this tab.

Step 6 Click **Show Advanced** to display additional port information. Table 10-4 describes the information.

Table 10-4 Ports Tab Field Descriptions

Field	Description
SubnetPrefix	Subnet prefix of the node.
NodeGUID	Global unique ID (GUID) of the node that includes the port.
Port	Local port number for this port.
LID	16-bit base LID of this port.
State	State of the port, as follows: • noStateChange • sleep • polling • disabled • portConfigurationTraining • linkup • linkErrorRecovery • reserved • active • down
LinkWidthActive	Active link width. Used in conjunction with LinkSpeedActive to determine the link rate between two nodes. The value appears as 1x, 4x, or 12x.
MKey	64-bit management key for this port. See section 14.2.4, “Management Key” and 3.5.3, “Keys,” in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
GID Prefix	64-bit Global identifier prefix for this port. The subnet manager assigns this prefix based upon the port routes and the rules for local identifiers. See section 4.1.3, “Local Identifiers,” in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
MasterSmLID	16-bit base LID of the master subnet manager managing this port.

Table 10-4 Ports Tab Field Descriptions (continued)

Field	Description
CapMask	The capability mask identifies the functions that the host supports. 32-bit bitmask that specifies the supported capabilities of the port. A bit value of 1 (one) indicates a supported capability. The bits are 0, 11-15, 18, 21-31 (Reserved and always 0.), 1 IsSM, 2 IsNoticeSupported, 3 IsTrapSupported, 4 IsResetSupported, 5 IsAutomaticMigrationSupported, 6 IsSLMappingSupported, 7 IsMKeyNVRAM (supports M_Key in NVRAM), 8 IsPKeyNVRAM (supports P_Key in NVRAM), 9 Is LED Info Supported, 10 IsSMdisabled, 16 IsConnectionManagementSupported, 17 IsSNMPTunnelingSupported, 19 IsDeviceManagementSupported, 20 IsVendorClassSupported.Values are expressed in hexadecimal.
DiagCode	16-bit diagnostic code. See section 14.2.5.6.1 “Interpretation of Diagcode,” in *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information. This field does not currently apply to your server switch.
MKeyLeasePeriod	Initial value of the lease-period timer, in seconds. The lease period is the length of time that the M_Key protection bits are to remain non-zero after a SubnSet (PortInfo) fails an M_Key check. After the lease period expires, clearing the M_Key protection bits allows any subnet manager to read (and then set) the M_Key. Set this field to 0 to indicate that the lease period never expires. See *InfiniBand Architecture®, Vol. 1, Release 1.1*, section 14.2.4, “Management Key.”
LinkWidthEnabled	Enabled link width (bandwidth). The value (an integer) indicates the enabled link-width sets for this port. The value can be one of the following: • no state change • 1x • 4x • 1x, 4x • 8x • 1x, 8x • 4x, 8x • 1x, 4x, 8x • 12x • 1x, 12x • 4x, 12x • 1x, 4x, 12x • 8x, 12x • 1x, 8x, 12x • 4x, 8x, 12x • 1x, 4x, 8x, 12x • reserved • linkwidthsupported value

Table 10-4 Ports Tab Field Descriptions (continued)

Field	Description
LinkWidthSupported	Supported link width. The value appears as one of the following: • 1x, • 1x, 4x • 1x, 4x, 8x • 1x, 4x, 12x, • 1x, 4x, 8x, 12x • reserved
LinkSpeedSupported	Supported link speed. The value appears as one of the following: • sdr • sdr, ddr
PhyState	Indicates the physical state of the port, whether or not electricity flows between nodes and that they can perform a handshake. The value appears as noStateChange, sleeping, polling, disabled, portConfigurationTraining, linkup, or linkErrorRecovery. The state, upon power-up, defaults to polling.
LinkDownDefState	Default LinkDown state to return to. The value appears as noStateChange, sleeping, or polling. See section 5.5.2, "Status Outputs (MAD GET)," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
MKeyProtBits	Management key protection bits for the port. The bits are 0, 1, 2, and 3. See section 14.2.4.1, "Levels of Protection," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
LMC	Local-identifier mask control (LMC) for multi-path support. A LMC resides on each channel adapter and router port on the subnet. It provides multiple virtual ports within a single physical port. The value of the LMC specifies the number of path bits in the LID. A value of 0 (zero) indicates one LID can apply to this port. See sections 3.5.10, "Addressing," and 4.1.3, "Local Identifiers," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
LinkSpeedActive	Speed of an active link. The value appears as one of the following: • sdr • ddr
LinkSpeedEnabled	Maximum speed that the link can handle. The value appears as one of the following: • sdr • ddr • sdr, ddr
NeighborMTU	Active maximum transmission unit enabled on this port for transmit. Check the MTUCap value at both ends of every link and use the lesser speed. The value appears as 256, 512, 1024, 2048, or 4096.
MasterSmSL	Administrative service level required for this port to send a non-SMP message to the subnet manager.
VLCap	Maximum range of data virtual lanes supported by this port. The value appears as vl0, vl0-Vl1, vl0-Vl3, vl0-Vl7, or vl0-Vl14. See also oper-VL. Each port can support up to 15 virtual lanes (VLs 0 - 15). The VL-cap field displays the range of those lanes (for example, lanes 0 - 7) that the port currently supports.

Table 10-4 Ports Tab Field Descriptions (continued)

Field	Description
VLHighLimit	Maximum high-priority limit on the number of bytes allowed for transmitting high-priority packets when both ends of a link operate with multiple data virtual-lanes. Used with the virtual-lane arbitration table. The maximum high-limit matches the VLArbHighSap on the other side of the link and then negotiating downward.
VLArbHighCap	Highest arbitration value allowed by the arbiter in determining the next packet in a set of packets to send across the link. Used with the virtual-lane arbitration table and specified as a VL/Weight pair. See section 14.2.5.9, "VL Arbitration Table," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
VLArbLowCap	Lowest arbitration value allowed by the arbiter in determining the next packet in a set of packets to send across the link. Used with the virtual-lane arbitration table and specified as a VL/Weight pair. See section 14.2.5.9, "VL Arbitration Table," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
MTUCap	Used in conjunction with NeighborMTU to determine the maximum transmission size supported on this port. The lesser of MTUCap and NeighborMTU determines the actual MTU used. The value appears as 256, 512, 1024, 2048, or 4096.
VLStallCount	Number of sequentially dropped packets at which the port enters a VLStalled state. The virtual lane exits the VLStalled state (8 * HLL) units after entering it. See section 18.2.5.4, "Transmitter Queuing," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for a description of HLL.
HOQLife	Maximum duration allowed to packets at the head of a virtual-lane queue. Used with VLStallCount to determine the outgoing packets to discard.
OperVL	Administrative limit for the number of virtual lanes allowed to the link. Do not set this above the VLCap value. The value appears as vl0, vl0-Vl1, vl0-Vl3, vl0-Vl7, or vl0-Vl14.
InPartEnforce	Boolean value that indicates whether or not to support optional partition enforcement for the packets that were received by this port. No default value applies.
OutPartEnforce	Boolean value that indicates whether or not to support optional partition enforcement for the packets transmitted by this port. No default value applies.
InFilterRawPktEnforce	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets that were received by this port. No default value applies.
OutFilterRawPktEnforce	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets transmitted by this port. No default value applies.
MKeyViolation	Number of subnet management packets (SMPs) that have been received on this port with invalid M_Keys since initial power up or the last reset. See section 14.2.4, "Management Key," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
PKeyViolation	Number of subnet management packets that have been received on this port with invalid P_Keys since initial power up or the last reset. See section 9.2.7, "Partition Key (P_KEY)," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.

Table 10-4 Ports Tab Field Descriptions (continued)

Field	Description
QKeyViolation	Number of subnet management packets that have been received on this port with invalid Q_Keys since initial power up or the last reset. See section 10.2.4, "Q Keys," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
GUIDCap	Number of GUID entries allowed for this port in the port table. Any entries that exceed this value are ignored on write and read back as zero. See section 14.2.5.5, "GUIDCap," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
SubnetTimeout	Maximum propagation delay allowed for this port to reach any other port in the subnet. This value also affects the maximum rate at with traps can be sent from this port. Switch configuration affects delay. Requestors can use this parameter to determine the interval to wait for a response to a request. Duration matches (4.096 ms * 2^SubnetTimeout).
RespTime	Maximum time allowed between the port reception of a subnet management packet and the transmission of the associated response. See section 13.4.6.2, "Timers and Timeouts," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
LocalPhyError	Threshold at which ICRC, VCRC, FCCRC, and all physical errors result in an entry into the BAD PACKET or BAD PACKET DISCARD states of the local packet receiver. See section 7.12.2, "Error Recovery Procedures," *InfiniBand Architecture®, Vol. 1, Release 1.1*, for more information.
LocalOverrunError	Threshold at which the count of buffer overruns, across consecutive flow-control update periods, result in an overrun error. A possible cause of such errors is when an earlier packet has physical errors and the buffers are not immediately reclaimed.

Viewing Switches

To view the switches in the topology view, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column of additional InfiniBand devices to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Click **Details**.

The InfiniBand Subnet Details window opens.

Step 5 Click the **Switches** tab.

Table 10-5 describes the fields in this tab.

Table 10-5 Switches Tab Field Descriptions

Field	Description
SubnetPrefix	Subnet prefix of the node.
NodeGUID	Global unique ID (GUID) of the node that includes the switch.
LinearFdbCap	Number of entries supported in the Linear Unicast Forwarding table. Zero indicates that there is no Linear Forwarding Database.
RandomFdbCap	Number of entries supported in the Random Unicast Forwarding table. Zero indicates that there is no Random Forwarding Database.
McastFdbCap	Number of entries supported in the Multicast Forwarding table.
LinearFdbTop	Indicates the top of the linear forwarding table. Packets received with unicast DLIDs greater than this value are discarded by the switch. This component applies only to switches that implement linear forwarding tables and is ignored by switches that implement random forwarding tables.
DefaultPort	Forward to this port all the unicast packets from the other ports where DLID does not exist in the random forwarding table.
DefPriMcastPort	Forward to this port all the multicast packets from the other ports where DLID does not exist in the forwarding table.
DefNonPriMcastPort	Forward to this port all the multicast packets from the smDefPriMcastPort port where DLID does not exist in the forwarding table.
LifeTimeValue	Time a packet can live in the switch.
PortStateChange	Identifies whether or not the port is in transition.
LIDPerPort	Number of LID/LMC combinations that may be assigned to a given external port for switches that support the random forwarding table.
PartitionEnfCap	Number of entries in this partition enforcement table per physical port. Zero indicates that partition enforcement is not supported by the switch.
InEnfCap	Indicates switch is capable of partition enforcement on received packets.
OutEnfCap	Indicates switch is capable of partition enforcement on transmitted packets.
InFilterRawPktCap	Indicates switch is capable of raw packet enforcement on received packets.
OutFilterRawPktCap	Indicates switch is capable of raw packet enforcement on transmitted packets.

Viewing Neighboring Ports

To view neighboring ports in the topology view, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Click **Details**.

The InfiniBand Subnet Details window opens.

Step 5 Click the **Neighbors** tab.

Table 10-6 describes the fields in this tab.

Table 10-6 Neighbors Tab Field Descriptions

Field	Description
SubnetPrefix	Used to identify InfiniBand subnet in which this InfiniBand node is located.
LocalNodeGuid	Global unique ID (GUID) of the InfiniBand node.
LocalPortId	Port ID of the InfiniBand node.
LocalNodeType	Identifies the node type of the InfiniBand node as follows. • channelAdapter • switch
RemoteNodeGuid	Global unique ID (GUID) of the remote InfiniBand node.
RemotePortId	Port ID of the remote InfiniBand node.
RemoteNodeType	Identifies the remote InfiniBand node's node-type, as follows: • channelAdapter • switch
LinkState	Identifies the state of the link connecting the neighbors, as follows: • noStateChange • down • initialize • active
LinkWidthActive	Width of the link connecting the neighbors.

Viewing Subnet Management Agents

These topics describe how to view Subnet Manager Agent details:

- Viewing the Subnet Manager Agent Partition Details, page 10-19
- Viewing the Subnet Manager Agent SLVL Map, page 10-20

Viewing Subnet Manager Node Details

To view Subnet Manager Agent node details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

Step 5 The Internal InfiniBand Topology window opens.

Step 6 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 7 Click the **Nodes** tab.

Table 10-7 describes the fields in this tab.

Table 10-7 Nodes Tab Field Descriptions

Field	Description
Guid	Subnet prefix of this InfiniBand subnet.
BaseVersion	Supported base management datagram version.
ClassVersion	Supported subnet management class.
Type	Type of node being managed: channelAdapter or switch
PortGuid	GUID of this port. One port within a node can return the nodeGUID as its PortGUID if the port is an integral part of the node and is not field-replaceable.
PartitionCap	Number of entries in the partition table for CA, router, and the switch management port. This is at a minimum set to 1 for all nodes including switch.
DeviceId	Device ID information as assigned by the device manufacturer.
Revision	Device revision assigned by manufacturer.
LocalPortNum	The link port number that this SNMP packet came in on.
VendorId	Device vendor ID, per IEEE.
TrapBuffer	Special-purpose string buffer for InfiniBand Trap Data.
String	Description of the node.
NumPorts	Number of physical ports on this node.

Viewing Subnet Manager Switch Details

To view Subnet Manager Agent switch details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

Step 6 The Subnet Manager Agents window opens.

Step 7 Click the **Switches** tab.

Table 10-8 describes the fields in this tab.

Table 10-8 Switches Tab Field Descriptions

Field	Description
Guid	Global unique ID of the switch.
LftTop	Top of the linear forwarding table. Packets received with unicast DLids greater than this value are discarded by the switch. This component applies only to switches that implement linear forwarding tables and is ignored by switches that implement random forwarding tables.
DefaultPort	Forward to this port all the unicast packets from the other ports where DLID does not exist in the random forwarding table.
DefMcastPriPort	Forward to this port all the multicast packets from the other ports where DLID does not exist in the forwarding table.
DefMcastNPPort	Forward to this port all the multicast packets from the Default Primary port where DLID does not exist in the forwarding table.
LifeTimeValue	Time that a packet can live in the switch.
PortStateChange	Set to one when the PortState component in the PortInfo of any ports transitions from Down to Initialize, Initialize to Down, Armed to Down, or Active to Down as a result of link state machine logic. Changes in Portstate resulting from SubnSet do not change this bit. This bit is cleared by writing one; writing zero is ignored.
LidsPerPort	Number of LID/LMC combinations that may be assigned to a given external port for switches that support the random forwarding table.

Viewing Subnet Manager Agent Switch Cap Details

To view Subnet Manager Agent switch cap details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **Switch Cap** tab.

Table 10-9 describes the fields in this tab.

Table 10-9 Switch Cap Tab Field Descriptions

Field	Description
LftCap	Number of entries supported in the linear unicast forwarding table.
RftCap	Number of entries supported in the random unicast forwarding table. RandomFDBCap = 0 indicates that there is no random forwarding database.
MftCap	Number of entries supported in the multicast forwarding table.
PartitionEnfCap	Number of entries in the partition enforcement table per physical port. Zero indicates that partition enforcement is not supported by the switch.
InboundEnfCap	Indicates switch is capable of partition enforcement on received packets.
OutboundEnfCap	Indicates switch is capable of partition enforcement on transmitted packets.
FilterRawPktInCap	Indicates switch is capable of raw packet enforcement on received packets.
FilterRawPktOutCap	Indicates switch is capable of raw enforcement on transmitted packets.

Viewing Subnet Manager Agent Ports(1) Details

To view Subnet Manager Agent port details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column of any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **Ports (1)** tab.

Table 10-10 describes the fields under this tab.

Table 10-10 Ports (1) Tab Field Descriptions

Field	Description
NodeGuid	64-bit GUID of the node that contains this port.
IbPort	Local port number of this port (relative to a particular node).
MKey	64-bit management key for this port.
GidPrefix	64-bit global ID prefix for this port.
Lid	16-bit base LID of this port.
MasterSMLid	16-bit base LID of the master Subnet Manager that is managing this port.
CapabilityMask	Supported capabilities of this node are as follows: • 0: Reserved, shall be zero • 1: IsSM • 2: IsNoticeSupported • 3: IsTrapSupported • 4: IsResetSupported • 5: IsAutomaticMigrationSupported • 6: IsSLMappingSupported • 7: IsMKeyNVRAM • 8: IsPKeyNVRAM • 9: IsLEDInfoSupported • 10: IsSMDisabled • 11-15: Reserved, shall be zero • 16: IsConnectionManagerSupported • 17: IsSNMPTunnelingSupported • 18: Reserved, shall be zero • 19: IsDeviceManagementSupported • 20: IsVendorClassSupported • 21-31: Reserved, shall be zero
DiagCode	Port diagnostic code.
MKeyLeasePeriod	Timer value used to indicate how long the M_Key protection bits are to remain nonzero after a SubnSet(PortInfo) fails an M Key check. The value of the timer indicates the number of seconds for the lease period.
LocalPortNum	Local port number.
LinkWidthEnabled	Enabled link width (1x, 4x, or 12x).
LinkWidthSupported	Supported link width.

Table 10-10 Ports (1) Tab Field Descriptions (continued)

Field	Description
LinkWidthActive	Currently active link width.
LinkSpeedSupported	Supported link speed (in Gbps).
State	State of the port is as follows: • noStateChagne • down • initialize • armed • active
PortPhys	State of the physical port is as follows: • noStateChange(0), • sleep • polling • disabled • portConfigurationTraining • linkup • linkErrorRecovery • reserved • linkDownDef
LinkDownDef	Port physical state link down.
MKeyProtectBits	Determines MADheader behavior.
LMC	LID mask for multipath support.
LSActive	Current active link speed.
LSActiveEnabled	Enabled link speed.
NeighborMTU	Active maximum MTU enabled on this port for transmission.
MasterSMSL	Administrative SL of the master Subnet Manager that is managing this port.

Viewing Subnet Manager Agent Ports (2) Details

To view extended Subnet Manager Agent port details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **Ports (2)** tab.

Table 10-11 describes the fields in this tab.

Table 10-11 Ports (2) Tab Field Descriptions

Field	Description
NodeGuid	64-bit GUID of the node that contains this port.
IbPort	Local port number of this port (relative to a particular node).
VLCap	Virtual lanes supported on this port.
VLHighLimit	Limit of high priority component of VL arbitration table.
VLArbitrationHighCap	VL/Weight pairs supported on this port in the smVLArbTable for high priority.
VLArbitrationLowCap	VL/Weight pairs supported on this port in the smVLArbTable for low priority.
MTUCap	Maximum MTU supported by this port.
VLStallCount	Number of sequential packets dropped that caused the port to enter the VLStalled state.
HoQLife	Time that a packet can live at the head of a VL queue.
OpVLs	Virtual Lanes operational on this port.
PkeyEnfIn	Indicates support of optional partition enforcement on packets received from this port.
PkeyEnfOut	Indicates support of optional partition enforcement on packets transmitted from this port.
FilterRawPktIn	Indicates support of optional raw packet enforcement on raw packets received from this port.
FilterRawPktOut	Indicates support of optional raw packet enforcement on raw packets transmitted from this port.
MKeyViolations	Number of SMP packets that were received on the port and had an invalid M_Key, since power on or reset.
PKeyViolations	Number of packets that were received on the port and had an invalid P_Key, since power on or reset.
QKeyViolations	Number of packets that have been received on the port that have had an invalid Q_Key, since power on or reset
GuidCap	Number of GUID entries supported in the GUIDInfo attribute for this port.
SubnetTimeout	Maximum expected subnet propagation delay.
RespTimeValue	Expected maximum time between the port reception of an SMP and the transmission of the associated response.

Table 10-11 Ports (2) Tab Field Descriptions (continued)

Field	Description
LocalPhysErr	Threshold value. When the count of marginal link errors exceeds this threshold, the local link integrity error is detected.
OverrunErr	Overrun threshold value. When the count of buffer overruns exceeds the threshold, an excessive buffer overrun error occurs.

Viewing Subnet Manager Multicast Details

To view Subnet Manager Agent multicast details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **Mcast** tab.

Table 10-12 describes the fields in this tab.

Table 10-12 Mcast Tab Field Descriptions

Field	Description
NodeGuid	Global unique ID of the node.
TableBlockIndex	Index into the multicast block table: this index starts from 1 rather than 0.
TableBlock	List of 32 PortMask Block Elements. 16 bits starting at position 16*p of the port mask are associated with the particular LID. An incoming packet with this LID is forwarded to all ports for which the bit in the port mask is set to 1. An invalid LID is indicated with an all zero PortMask.

Viewing Subnet Manager Agent Linear Forwarding Table Details

To view Subnet Manager Agent linear forwarding table details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **Linear Forwarding** tab.

Table 10-13 describes the fields in this tab.

Table 10-13 Linear Forwarding Tab Field Descriptions

Field	Description
NodeGuid	Global unique ID of the node.
BlockIndex	Index into the linear forwarding table; this index starts from 1 rather than 0.
Block	Linear forwarding table block.

Viewing the Subnet Manager Agent Partition Details

To view Subnet Manager Agent partition details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **PKey** tab.

Table 10-14 describes the fields in this tab.

Table 10-14 PKey Tab Field Descriptions

Field	Description
NodeGuid	Global unique ID of the node.
IbPort	Port number.
Index	PKEY table index.
TableVector	GUID assigned by the Subnet Manager on the subnet.

Viewing the Subnet Manager Agent SLVL Map

To view Subnet Manager Agent SLVL details, follow these steps:

Step 1 From the InfiniBand menu, choose **Topology** View.

The Specify Cisco Devices dialog box opens.

Step 2 (Optional) Check the check box in the Enabled column for any additional InfiniBand devices that you want to add to the Topology View display.

Step 3 Click **OK**.

The InfiniBand Topology window appears.

Step 4 Double-click a server switch icon.

The Internal InfiniBand Topology window opens.

Step 5 Click **SMAs**.

The Subnet Manager Agents window opens.

Step 6 Click the **SLVL Map** tab.

Table 10-15 describes the fields in this tab.

Table 10-15 SLVL Map Tab Field Descriptions

Field	Description
NodeGuid	Global unique ID of the node.
InIbPort	Ingress port number.
OutIbPort	Egress port number.
Sl#toVI	SL# to VL mapping.

CHAPTER 11

InfiniBand Device Management Tasks

Device Management features are available only on I/O chassis (Cisco SFS 3001 and Cisco SFS 3012).

These topics describe the InfiniBand device management menu tasks for Element Manager:

Note See Appendix A for information to familiarize you with the InfiniBand technology. For hardware-specific information, consult the relevant hardware documentation.

Viewing IOUs

To view the I/O Units (IOUs) on your device, follow these steps:

Step 1 From the InfiniBand menu, choose **Device Management (tabular format)**.

The Device Manager window opens.

Step 2 Click the **IOU** tab.

IOU details appear in the right pane. Table 11-1 describes the fields in this pane.

Table 11-1 IOU Tab Field Descriptions Pane

Field	Description
Change ID	Cumulative number of changes to the controller list since the device last booted.
Max Controllers	Maximum number of controllers that your device can support.
Diag Device ID	All device IDs appear as 1.
Option ROM	Indicates the presence or absence of Option ROM.
Controllers	Lists each slot on your device that can potentially contain a controller and identifies whether or not a controller resides in that slot.

Viewing IOCs

To view the I/O controllers (IOCs) on your device, follow these steps:

Step 1 From the InfiniBand menu, choose **Device Management (tabular format)**.

The Device Manager window opens.

Step 2 Click the **IOC** tab.

A table of IOC details appears. Table 11-2 describes the fields in this display.

Table 11-2 IOCs Display Field Descriptions

Field	Description
GUID	GUID of the controller.
Vendor ID	Organization Unique Identifier (OUI) of the vendor.
Device ID	Vendor-assigned device identifier.
Device Version	Vendor-assigned device version.
Subsystem Vendor ID	Vendor-assigned subsystem vendor identifier
Subsystem ID	Vendor-assigned subsystem identifier.
IOClass	I/O class that the IOC supports.
IOSubclass	Subclass of the I/O class protocol of the IOC.
Protocol	Standard protocol definition that the IOC supports.
Protocol Version	Protocol version that the IOC supports.
Send Msg Queue Depth	Maximum number of messages that the send message queue supports.
RDMA Read Queue Depth	Maximum depth of the per-channel RDMA Read Queue.
Send Msg Size	Maximum size, in bytes, of send messages.
RDMA transfer size	Maximum size, in bytes, of outbound RDMA transfers that the IOC initiates.
Controller Op Cap	Integer value (from 8 cumulative bits) between 1 and 255 that represents the operation type(s) that the IOC supports. • Bit 0: ST; Send Messages To IOCs • Bit 1: SF; Send Messages From IOCs • Bit 2: RT; RDMA Read Requests To IOCs • Bit 3: RF; RDMA Read Requests From IOCs • Bit 4: WT; RDMA Write Requests To IOCs • Bit 5: WF; RDMA Write Requests From IOCs • Bit 6: AT; Atomic Operations To IOCs • Bit 7: AF; Atomic Operations From IOCs
Service Entries	Number of services that the IOC provides.

Viewing IOC Services

To view the IOC services on your device, follow these steps:

Step 1 From the InfiniBand menu, choose **Device Management (tabular format)**.

Step 2 The Device Manager window opens.

Step 3 Click the **IOC Services** tab.

A table of IOC Services details appears. Table 11-3 describes the fields in this table.

Table 11-3 IOC Services Table Field Descriptions

Field	Description
IOC GUID	GUID of the node that provides the service.
Service Name	ASCII identifier of the service.
Service ID	Numeric identifier that nodes use to call the service.

CHAPTER 12

Ethernet Menu Tasks

These topics describe the Ethernet menu tasks for Element Manager:

Note The instructions in this chapter apply only to server switches that run Ethernet gateways.

Viewing and Adding Addresses to the Static ARP Table

These topics describe how to view and manage the static ARP table:

Viewing the ARP Table

To view the static ARP table, from the Ethernet menu, choose **ARP**.

The ARP window opens and displays the static ARP table. Table 12-1 describes the fields in this table.

Table 12-1 ARP Table Field Descriptions

Field	Description
Port	Port (in slot#port# format) on your server switch to which the host connects.
NetAddress	IP address of the host.
PhysAddess	MAC address of the host.
Type	Type of route between the host and your server switch, either static or dynamic.

Adding a Static Address to the ARP Table

To add a static address to the ARP table, follow these steps:

Step 1 From the Ethernet menu, choose **ARP**.

The ARP window opens and displays the static ARP table.

Step 2 Click **Insert Ethernet**.

The Insert static Ethernet ARP window opens.

Step 3 Click the **...** button next to the Port field.

The choose Port window opens.

Step 4 Check the check box of the Ethernet gateway port to which you want to assign the new entry, and then click **OK**.

Step 5 Enter the IP address of the static host in the Net Address field.

Step 6 Enter the MAC address of the static host in the MAC field, and then click **Insert**.

Viewing and Managing Ethernet Routes

These topics describe how to view and manage Ethernet routes:

Viewing Ethernet Routes

To view Ethernet routes, from the Ethernet menu, choose **Routes**.

The Routes window opens. Table 12-2 describes the fields in this window.

Table 12-2 Routes Window Field Descriptions

Field	Description
Dest	Destination IP address of the route.
Mask	Subnet mask of the route.
NextHop	IP address of the next hop on the Ethernet route (address of the Ethernet router).
Port	Ethernet gateway port of the route.
Type	Identifies the type of route as direct or indirect.
Proto	Protocol that the route runs.
NextHopAS	Autonomous System Number of the next hop.

Creating an Ethernet Route

To create an Ethernet route, follow these steps:

Step 1 From the Ethernet menu, choose **Routes**.

The Routes window opens.

Step 2 Click **Insert**.

The Insert Routes window opens.

Step 3 Enter the destination IP address in the Dest field.

Step 4 Enter the subnet mask in the Mask field.

Step 5 Enter the IP address of the next hop in the NextHop field, and then click **Insert**.

Deleting an Ethernet Route

To delete an Ethernet route, follow these steps:

Step 1 From the Ethernet menu, choose **Routes**.

The Routes window opens.

Step 2 Click the route to delete, and then click **Delete**.

Viewing IP Addresses

To view IP addresses, from the Ethernet menu, choose **IP Addresses**.

The IP Addresses window opens. Table 12-3 describes the fields in this window.

Table 12-3 IP Addresses Window Field Descriptions

Field	Description
Port	Index value that uniquely identifies the interface to which this entry is applicable.
Address	IP address to which the addressing information of this entry pertains.
Netmask	Subnet mask associated with the IP address of this entry.
BcastAddrFormat	IP broadcast address format used on this interface.
ReasmMaxSize	Size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
Type	Identifies the address as a primary or backup address.
Status	Identifies the port as active or backup.

Viewing and Managing Trunk Groups

These topics describe how to view and manage trunk groups:

- Viewing Trunk Groups, page 12-4
- Creating a Trunk Group, page 12-5
- Deleting a Trunk Group, page 12-5
- Editing a Trunk Group, page 12-5

Viewing Trunk Groups

To view the trunk groups on your server switch, from the **Ethernet** menu, choose **Trunking**.

The Trunking window opens. Table 12-4 describes the fields in this window.

Table 12-4 Trunking Window Field Descriptions

Field	Description
ID	Trunk group identifier.
Name	Trunk group name.
Port Members	Physical Ethernet gateway ports that belong to this trunk group.
Distribution Type	Packet forwarding distribution algorithm of the trunk group.
Enabled	Identifies the trunk group as enabled or disabled.
MTU	Maximum transmission unit of the trunk group.
MAC Address	MAC address assigned to this trunk group.
IfIndex	Logical port identifier that represents the trunk group.

Creating a Trunk Group

To create a trunk group, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 Click **Insert**.

The Insert Trunk Groups window opens.

Step 3 In the ID field, enter an integer value (between 1 and 256).

Step 4 In the Name field, enter a name, with ASCII characters.

Step 5 Click the **...** button in the Port Members field.

The choose Ports window opens.

Step 6 Check the check box of any port that you want to add to the trunk group. Uncheck any check box that you want to omit from the group. Click **OK**.

Step 7 In the Distribution Type field, click the radio button of a distribution type.

Step 8 (Optional) Check the **Enabled** check box to enable the new group when you create it. To disable the new group, uncheck the check box.

Step 9 Click **Insert**.

The new group appears as a row in the Trunking window.

Deleting a Trunk Group

To delete a trunk group, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 Click the entry of the trunk group that you want to delete, and then click **Delete**.

Editing a Trunk Group

Trunk groups can be edited as follows:

- Changing a Trunk Group Name, page 12-6
- Adding or Removing Physical Ethernet Gateway Ports from a Trunk Group, page 12-6
- Changing the Distribution Type of a Trunk Group, page 12-6
- Enabling or Disabling a Trunk Group, page 12-7

Changing a Trunk Group Name

To change a trunk group name, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 Double-click the cell in the Name column of the entry with a name that you want to change.

The cell becomes editable.

Step 3 Enter the new trunk group name, and then press the **Enter** key.

Step 4 Click **Apply**.

Note You can make multiple changes before you click **Apply**, but you must click it to make the changes in the configuration file on the server switch.

Adding or Removing Physical Ethernet Gateway Ports from a Trunk Group

To add or remove physical Ethernet gateway ports from a trunk group, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 Double-click the cell in the Port Members column of the entry to which you want to add or remove ports.

The choose Ports window opens.

Step 3 In the Choose Ports window, check the check boxes of ports to add to the group. Uncheck the boxes of ports to remove. Click **OK**.

Step 4 Click **Apply**.

Note You can make multiple changes before you click Apply, but you must click it to make the changes in the configuration file on the server switch.

Changing the Distribution Type of a Trunk Group

To change the distribution type of a trunk group, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 In the Distribution Type column, click the cell of the trunk group with a distribution type that you want to change.

A drop-down menu appears.

Step 3 From the drop-down menu, choose a new distribution type.

Step 4 Click **Apply**.

Note You can make multiple changes before you click Apply, but you must click it to make the changes in the configuration file on the server switch.

Enabling or Disabling a Trunk Group

To enable or disable a trunk group, follow these steps:

Step 1 From the Ethernet menu, choose **Trunking**.

The Trunking window opens.

Step 2 Click the cell in the Enabled column of the trunk group with the enabled/disabled status that you want to change.

A drop-down menu appears.

Step 3 From the drop-down menu, choose **true** (to enable) or **false** (to disable).

Step 4 Click **Apply**.

Note You can make multiple changes before you click Apply, but you must click it to make the changes in the configuration file on the server switch.

Viewing and Managing Bridge Groups

These topics describe how to view and manage bridge groups:

Viewing Bridge Groups

To view the bridge groups on the server switch, from the Ethernet menu, choose **Bridging**.

The Bridging window opens. Table 12-5 describes the fields in this window.

Table 12-5 Bridging Window Field Descriptions

Field	Description
ID	Unique numeric identifier of the bridge group.
Name	Name in ASCII characters, of the bridge group.
Ethernet Port	Ethernet interface that is assigned to this bridge group. A value of zero (0) means that no interface is currently assigned.
IB Port	InfiniBand interface that is assigned to this bridge group. A value of zero (0) means that no interface is currently assigned.
Broadcast Forwarding	Configures whether or not this bridge group should forward broadcast packets. Enabling broadcast forwarding can cause broadcast storms in a network if the network is not configured properly.
Broadcast Forwarding Mode	Active broadcast forwarding mode.
Loop Protection Method	Loop protection method of this bridge group.
IP Multicast	Specifies if the group forwards IP-V4 multicast packets.
IP Multicast Mode	Active IP multicast mode.
Redundancy Group	Redundancy group to which this bridge group is assigned.
Oper Failover Priority	Active failover priority of the bridge group.
IP Address	IP address of the bridge group.
Gratuitous IGMP	Displays Enabled if gratuitous IGMP is set, otherwise displays Disabled.
Gratuitous IGMP Mode	Active gratuitous IGMP mode.
IGMP Version	Active IGMP version, v1, v2, or v3.
IGMP Version Mode	Active IGMP version mode.

Table 12-5 Bridging Window Field Descriptions (continued)

Field	Description
Directed Broadcast	Indicates whether directed broadcasting is enabled for the bridge group.
Directed Broadcast Mode	Active directed-broadcast mode.

Creating a Bridge Group

To create a bridge group, follow these steps:

Step 1 From the Ethernet menu, choose **Bridging**.

The Bridging window opens.

Step 2 Click **Add**.

The Add Bridge Group window opens.

Step 3 (Optional) In the ID field, enter an integer to assign a numeric identifier to the bridge group.

Element Manager automatically populates this field.

Step 4 In the Name field, enter a plain-text identifier of ASCII characters.

Step 5 Click the **Groups** tab.

Step 6 In the Ethernet Port field, click **Select**.

The Bridge Port window opens.

Step 7 From the Port drop-down menu, choose the Ethernet gateway port to assign to the bridge group.

Step 8 (Optional) In the VLAN field, enter the VLAN of the Ethernet gateway port to assign to the bridge group.

Step 9 Click **OK**.

Step 10 In the InfiniBand Port field, click **Select**.

The Bridge Port window opens.

Step 11 From the Port drop-down menu, choose the internal InfiniBand port on the Ethernet gateway to assign to the bridge group.

Step 12 In the P_Key field, enter the partition key of the partition to add the internal port.

Step 13 Click **OK**.

Step 14 (Optional) In the Broadcast Forwarding field, check the **Enabled** check box to enable broadcast forwarding.

Step 15 In the Loop Protection Method field, choose **one** or **none** from the drop-down menu.

Currently, only one method of loop protection is supported.

Step 16 (Optional) In the IP Multicast field, check the **Enabled** check box to enable IP multicast forwarding.

Step 17 (Optional) In the IP Address field, enter an IP Address for the bridge group.

Step 18 (Optional) Check the **Gratuitous IGMP** check box to enable gratuitous IGMP for the bridge group.

Enable this feature when IGMP snooping is enabled on the Ethernet switches connected to the Ethernet gateway.

Step 19 (Optional) From the IGMP Version drop-down menu, choose an IGMP version for the bridge group.

The IGMP version must be set to correspond to the version used by the hosts and routers bridged by this bridge group. It is used by gratuitous IGMP to generate reports and might have additional future uses.

Step 20 (Optional) In the Directed Broadcast field, check the **Enabled** check box to enable directed broadcasting for the bridge group.

Directed broadcasting allows directed broadcast traffic from the remote subnet Ethernet host to be broadcast to the IB network bridged by this bridge group.

Step 21 Click **Add**.

Deleting a Bridge Group

To delete a bridge group, follow these steps:

Step 1 From the Ethernet menu, choose **Bridging**.

The Bridging window opens.

Step 2 Click the bridge group entry that you want to delete, and then click **Delete**.

Adding Bridge Forwarding to a Bridge Group

To add bridge forwarding to a group, follow these steps:

Step 1 From the Ethernet menu, choose **Bridging**.

The Bridging window opens.

Step 2 Click the bridge group to which you want to add bridge forwarding, and then click **Edit**.

The Edit Bridge Group window opens.

Step 3 Click the **Forwarding** tab.

Step 4 Click **Add**.

The Add Bridge Forwarding window opens.

Step 5 From the drop-down menu in the Port Type field, choose **eth** or **ib**.

Step 6 In the Destination Address field, enter the destination IP address.

Step 7 In the Destination Length field, enter an integer value from 0 to 32.

Step 8 In the Next Hop field, enter the IP address of the next hop.

Step 9 In the Subnet Prefix field, enter the subnet prefix of the next hop.

Step 10 In the Prefix Length field, enter an integer value from 0 to 32.

Step 11 Click **Add**.

Adding a Subnet to a Bridge Group

To add an IPv4 subnet for bridging by a bridge group, follow these steps:

Step 1 From the Ethernet menu, choose **Bridging**.

The Bridging window opens.

Step 2 Click the bridge group to which you want to add a subnet, and then click **Edit**.

The Edit Bridge Group window opens.

Step 3 Click the **Subnet** tab.

Step 4 Click **Add**.

The Add Subnet window opens.

Step 5 In the Subnet Prefix field, enter an IPv4 subnet prefix.

Step 6 In the Prefix Length field, enter an integer value from 0 to 32.

Step 7 Click **Add**.

Viewing and Managing Redundancy Groups

These topics describe how to view and manage redundancy groups:

Viewing Redundancy Groups

To view the redundancy groups on your server switch, from the **Ethernet** menu, choose **Redundancy**. The Redundancy Groups window opens. Table 12-6 describes the fields in this window.

Table 12-6 Redundancy Groups Window Field Descriptions

Field	Description
Group ID	Unique numerical identifier of the redundancy group.
Name	ASCII-text name of the redundancy group.
Group P_Key	16-bit multicast partition key used by this redundancy group.
Load Balancing	Used to enable/disable load balancing for this redundancy group.
Bridge Group Members	Indicates the bridge groups that are assigned to this redundancy group.
Broadcast Forwarding	Displays true if broadcast forwarding is enabled, otherwise displays false.
IP Multicast	Displays true if multicast forwarding is enabled, otherwise displays false.

Table 12-6 Redundancy Groups Window Field Descriptions (continued)

Field	Description
Member Force Reelection	Displays true if the group is configured to reelect a new primary when a new member joins the redundancy group or an existing member comes online, otherwise displays false.
Directed Broadcast	Indicates whether directed broadcasting is enabled for the redundancy group.

Creating a Redundancy Group

To create a redundancy group, follow these steps:

Step 1 From the Ethernet menu, choose **Redundancy**.

The Redundancy Groups window opens.

Step 2 Click **Add**.

The Add Redundancy Group window opens.

Step 3 (Optional) In the ID field, enter an integer value. Element Manager automatically populates this field.

Step 4 Enter a name for the redundancy group in the Name field.

Step 5 (Optional) In the Load Balancing field, check the **Enabled** check box to apply load balancing to this redundancy group.

Step 6 (Optional) In the Broadcast Forwarding field, check the **Enabled** check box to apply broadcast forwarding to this redundancy group.

Applying broadcast forwarding temporarily overwrites the broadcast forwarding setting on all members of the redundancy group. Once a bridge group is removed from a redundancy group the original broadcast forwarding setting is restored.

Step 7 (Optional) In the IP Multicast field, check the **Enabled** check box to apply the multicast forwarding feature to this redundancy group.

Applying multicast forwarding temporarily overwrites the multicast forwarding setting on all members of the redundancy group. Once a bridge group is removed from a redundancy group the original multicast forwarding setting is restored.

Step 8 (Optional) In the Member Force Reelection field, check the **Enabled** check box to force the redundancy group to elect a new primary when a new member joins, or when an existing member comes online.

Step 9 (Optional) Check the **Gratuitous IGMP** check box to enable gratuitous IGMP for the redundancy group.

Gratuitous IGMP ap[plied to a redundancy group temporarily overwrites the gratuitous IGMP status on all bridge groups members of the redundancy group. Once a bridge group is removed from a redundancy group the original gratuitous IGMP status is restored.

Step 10 (Optional) From the IGMP Version drop-down menu, choose an IGMP version for the redundancy group.

This setting temporarily overwrites the IGMP version setting on all bridge groups members of the redundancy group. Once a bridge group is removed from a redundancy group the original IGMP version setting is restored.

Step 11 (Optional) In the Directed Broadcast field, check the **Enabled** check box to enable directed broadcasting for the redundancy group.

Directed broadcasting allows directed broadcast traffic from the remote subnet Ethernet host to be broadcast to the IB network bridged by this redundancy group.

Directed broadcast applied to a redundancy group temporarily overwrites the directed-broadcast setting on all bridge groups that are members of the redundancy group. Once a bridge group is removed from a redundancy group the original directed-broadcast setting is restored.

Step 12 Click **Add Member**.

The Add Member window opens.

Step 13 From the Bridge Group drop-down menu, choose a bridge group.

Step 14 Click **Add**.

The entry appears in the Members field.

Step 15 (Optional) Repeat Step 12 through Step 14 to add additional members.

Step 16 Click **Apply**.

Editing a Redundancy Group

To edit a redundancy group, follow these steps:

Step 1 From the Ethernet menu, choose **Redundancy**.

The Redundancy Groups window opens.

Step 2 Click the entry of the redundancy group to edit, and then click **Edit**.

The Edit Redundancy Group window opens.

Step 3 (Optional) In the Name field, change the name.

Step 4 (Optional) In the Load Balancing field, check or uncheck the **Enabled** check box to enable or disable load balancing for this redundancy group.

Step 5 (Optional) In the IP Multicast field, check or uncheck the **Enabled** check box to enable or disable multicast forwarding for this redundancy group.

Applying multicast forwarding temporarily overwrites the multicast forwarding setting on all members of the redundancy group. Once a bridge group is removed from a redundancy group the original multicast forwarding setting is restored.

Step 6 (Optional) In the Member Force Reelection field, check or uncheck the **Enabled** check box to enable or disable the forced election of a new primary when a new member joins the redundancy group, or when an existing member comes online.

Step 7 (Optional) Check or uncheck the **Gratuitous IGMP** check box to enable or disable gratuitous IGMP for the redundancy group.

Gratuitous IGMP ap[plied to a redundancy group temporarily overwrites the gratuitous IGMP status on all bridge groups members of the redundancy group. Once a bridge group is removed from a redundancy group the original gratuitous IGMP status is restored.

Step 8 (Optional) From the IGMP Version drop-down menu, choose an IGMP version for the bridge group.

This setting temporarily overwrites the IGMP version setting on all bridge groups members of the redundancy group. Once a bridge group is removed from a redundancy group the original IGMP version setting is restored.

Step 9 (Optional) In the Broadcast Forwarding field, check or uncheck **Enabled** to enable or disable broadcast forwarding for this redundancy group.

Applying broadcast forwarding temporarily overwrites the broadcast forwarding setting on all members of the redundancy group. Once a bridge group is removed from a redundancy group the original broadcast forwarding setting is restored.

Step 10 (Optional) In the Directed Broadcasting field, check the **Enabled** check box to enable directed broadcasting for the redundancy group.

Directed broadcasting allows directed broadcast traffic from the remote subnet Ethernet host to be broadcast to the IB network bridged by this redundancy group.

Directed broadcast applied to a redundancy group temporarily overwrites the directed-broadcast setting on all bridge groups that are members of the redundancy group. Once a bridge group is removed from a redundancy group the original directed-broadcast setting is restored.

Step 11 (Optional) Click a bridge group member, and then click **Remove** to remove a bridge group member.

Step 12 (Optional) Click **Add Member** to add a bridge group member. (See the "Creating a Redundancy Group" section on page 12-12.)

Step 13 Click **Apply**.

Deleting a Redundancy Group

To delete a redundancy group, follow these steps:

Step 1 From the Ethernet menu, choose **Redundancy**.

The Redundancy Groups window opens.

Step 2 Click the entry of the redundancy group that you want to delete, and then click **Remove**.

The Delete Redundancy Group window opens.

Step 3 Click **Yes**.

CHAPTER 13

FibreChannel Menu Tasks

These topics describe the FibreChannel menu tasks for Element Manager:

Note This chapter describes Fibre Channel storage tasks. For detailed information and configuration samples, see the *Cisco SFS 3000 Series Product Family Fibre Channel Gateway User Guide*.

Some FibreChannel menu options include edit icons. Table 13-1 describes those icons.

Table 13-1 SRP Navigation Icons

Icon	Description
	The Copy icon copies the contents of cell(s). Select another editable cell or multiple editable cells, and paste the content.
	The Paste icon places copied content into the cell or cells that you select. You can paste the content of one cell into multiple cells. You can paste the content of two side-by-side cells into multiple rows of side-by-side cells.
	The Reset icon returns cells to the values held before you edited them. **Note** You can only reset cells before you click Apply.

Viewing and Configuring Global SRP Attributes

These topics describe FibreChannel menu tasks for viewing and configuring global SRP attributes:

Viewing Global SRP Attributes

To view global SRP attributes, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Global** tab.

Table 13-2 describes the fields in the tab.

Table 13-2 Global Attribute Field Descriptions

Field	Description
DefaultGatewayPortMaskPolicy	Boolean value that indicates if ports allow new SRP initiators to communicate through the Fibre Channel interface card(s).
DefaultLunPolicy	Boolean value that indicates if new SRP initiators have immediate access to target LUNs.
DefaultItlHiMark	Maximum number of requests that can be sent per logical unit. This value, an integer, falls between 1 and 256. This value defaults to 16.
DefaultItlMaxRetry	Number of times that an initiator may send the same I/O to a logical unit. Increase the value if you expect heavy traffic, or increase the default-itl-min-io-timeout value. The value, an integer, falls between 1 and 100. The value defaults to 5.
DefaultItlMinIoTimeout	Maximum amount of time for a logical unit to accept I/O traffic. Increase this value if you use a known slow connection, or increase the default-itl-max-retry value. The value, an integer, falls between 1 and 1800. The value defaults to 10 seconds.
DefaultItlDynamicPathAffinity	Boolean value that indicates if the system maintains a preference for a specific path. If the number of outstanding I/O requests becomes excessive, or the path fails, the ITL uses an alternative path.

Table 13-2 Global Attribute Field Descriptions (continued)

Field	Description
DefaultItlDynamicGatewayPortLoadBalancing	Boolean value that indicates if data may be sent between the initiator and Fibre Channel target using both ports on the gateway interface. Port selection is based upon comparative I/O traffic. The controller attempts to distribute traffic equally between the ports. This feature runs by default.
DefaultItlDynamicGatewayPortFailover	Boolean value that indicates if the controller may select an alternate gateway interface port if the primary path fails. This feature does not run by default.
DefaultSeqItlHiMark	Default I/O high mark for a sequential device.
DefaultSeqItlMaxRetry	Default for the maximum number of retries for a sequential device.
DefaultSeqItlMinIoTimeout	Default for the maximum number of retries for a sequential device.
DefaultSeqItlDynamicPathAffinity	Default for the dynamic path affinity setting for a sequential device.
DefaultSeqItlDynamicGatewayPortLoadBalancing	Default of the dynamic path affinity setting for a sequential device.
DefaultSeqItlDynamicGatewayPortFailover	Boolean value that indicates if the controller may select an alternate storage port if the primary path fails. This feature does not run by default.

Configuring Global ITL Attributes

Note When you change global attributes, the new attributes do not apply to existing ITLs. Newly created ITLs have the new global attributes, but you must manually update existing ITLs to match the properties of the new ITLs.

To configure global ITL attributes, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Global** tab.

Step 3 Click one of these radio buttons in the DefaultGatewayPortMaskPolicy field to configure the gateway port mask policy:

- Click the **restricted** radio button to deny new initiators access to Fibre Channel gateway ports.
- Click the **nonRestricted** radio button to grant new initiators access to Fibre Channel gateway ports.

Step 4 In the DefaultLunPolicy field, click one of these radio buttons to configure the LUN mask policy:

- Click the **restricted** radio button to deny new initiators access to logical units.
- Click the **nonRestricted** radio button to grant new initiators access to logical units.

Step 5 Configure global defaults for nonsequential (random) storage devices as follows:

a. In the DefaultItlHiMark field, enter an integer value, between 1 and 256, to specify the maximum number of requests that Fibre Channel gateways send to individual logical units.

b. In the DefaultItlMaxRetry field, enter an integer value, between 1 and 100, to specify the number of times that an initiator may send the same I/O to a logical unit.

c. In the DefaultItlMinIoTimeout field, enter an integer value, between 1 and 1800, to specify the amount of time (in seconds) for an ITL to accept I/O traffic.

d. (Optional) Check the **DefaultItlDynamicPathAffinity** check box.

e. (Optional) Check the **DefaultItlDynamicGatewayPortLoadBalancing** check box.

f. (Optional) Check the **DefaultItlDynamicGatewayPortFailover** check box.

Step 6 Configure global defaults for sequential (tape) storage devices as follows:

a. In the DefaultSeqItlHiMark field, enter an integer value, between 1 and 256, to specify the maximum number of requests that Fibre Channel gateways will send to individual logical units.

b. In the DefaultSeqItlMaxRetry field, enter an integer value, between 1 and 100, to specify the number of times an initiator may send the same I/O to a logical unit.

c. In the DefaultSeqItlMinIoTimeout field, enter an integer value, between 1 and 1800, to specify the amount of time (in seconds) for an ITL to accept I/O traffic.

d. (Optional) Check the **DefaultSeqItlDynamicPathAffinity** check box.

e. (Optional) Check the **DefaultSeqItlDynamicGatewayPortLoadBalancing** check box.

f. (Optional) Check the **DefaultSeqItlDynamicGatewayPortFailover** check box.

Step 7 Click **Apply**.

Viewing and Configuring SRP Initiators

View or configure SRP initiators either in tabular format in the Element Manager SRP window or in modular format in the Storage Manager.

These topics describe the FibreChannel menu tasks for viewing and configuring SRP initiators:

Viewing SRP Initiators

To view SRP initiators in tabular format in the SRP window, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Initiators** tab.

Table 13-3 describes the fields in the tab.

Table 13-3 Initiators Table Field Descriptions

Field	Description
Guid	Global Identifier of the initiator.
Extension	GUID extension of the initiator.
Description	ASCII text identifier of the initiator.
Wwnn	Fibre Channel gateway-assigned world-wide node name of the initiator.
Credit	Maximum number of outstanding SRP requests for each initiator connection.
State	When an initiator logs in to a target, the gateway port through which the connection goes through is marked '1'B. Otherwise, the port is marked '0'B.
PkeyCount	Number of partitions of which the initiator is a member (maximum of 16).
Pkeys	Partition keys of the partitions of which the initiator is a member.
BootupTargetWwpn	World-wide port name of the target that the initiator boots by default.
BootupFcLunId	Identifier of the LU that contains the boot image that the initiator boots.
Action	Last initiator action. This can be any of the following: • none: initial state before the initiator takes any action • discoveritl: discover and create ITL entities for this initiator without the initiator logging in • autoBind: binds the initiator to its WWNN and WWPNs
Result	Result of the action in the Action column.
AltBootupTargetWwpn	World-wide port name of the alternate target that the initiator boots.
AltBootupFcLunId	Identifier of the LU that contains the alternate boot image that the initiator boots.

Configuring Existing SRP Initiators

To configure existing SRP initiators (hosts), follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Initiators** tab.

Step 3 Identify the initiator entry that you want to reconfigure and locate that entry in the Initiators table.

Step 4 (Optional) In the Description column, double-click the cell, and then edit the description.

Step 5 (Optional) In the Wwnn column, double-click the cell, and then edit the WWNN.

Note We strongly recommend that you never manually edit an existing world-wide node name.

Step 6 (Optional) In the Pkeys column, double-click the cell, and then edit the partition keys.

Note We strongly recommend that you never manually edit an existing partition key entry.

Step 7 (Optional) In the BootupTargetWwpn field double-click the cell, and enter a new boot target.

Step 8 (Optional) In the BootupFcLunId field, double-click the cell, and enter a new boot LUN.

Step 9 (Optional) Click the cell in the Action column and choose an action from the drop-down menu.

The action executes when you click **Apply** and the result appears in the Result column of the table.

Step 10 Click **Apply**.

Viewing and Managing SRP Initiators with Storage Manager

These topics describe how to view and manage SRP initiators with Storage Manager:

Viewing SRP Initiators with Storage Manager

To view SRP initiators with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **SRP Hosts** folder.

The SRP Hosts display appears in the right pane. Table 13-4 describes the fields in this pane.

Table 13-4 SRP Hosts Field Descriptions Pane

Field	Description
Host	Hostname of the initiator.
WWNN	Fibre Channel gateway-assigned world-wide node name of the initiator.
Ports Registered With	Fibre Channel gateway ports through which the initiator connects to storage.

Viewing General SRP Initiator Details with Storage Manager

To view general SRP initiator details with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Click the initiator with details that you want to view.

The details appear in the right pane. Table 13-5 describes the fields in this pane.

Table 13-5 Initiator Details Field Descriptions Pane

Field	Description
SRP Initiator ID	GUID and GUID extension of the initiator, separated by a forward-slash (/).
Ports Registered With	Fibre Channel gateway ports through which the initiator connects to storage.
WWNN	Fibre Channel gateway-assigned world-wide node name of the initiator.
Description	ASCII text identifier of the initiator.
Boot Target WWPN	World-wide port name of the target that the initiator boots by default.
Boot FC LUN	Identifier of the LU that contains the boot image that the initiator boots.

Table 13-5 Initiator Details Field Descriptions Pane (continued)

Field	Description
WWPNs	When you configure an initiator and autobind the initiator to a WWNN and to WWPNs, autobinding creates virtual WWPNs for each possible Fibre Channel gateway port that could potentially appear on the server switch. • The Slot/Port column of the WWPNs table displays all of the potential Fibre Channel gateway ports on the chassis. • The WWPN column of the WWPNs table displays the WWPN that autobinding created for each possible physical Fibre Channel gateway port. Storage devices use these WWPNs to communicate with the initiator. • The Fibre Channel Address column of the WWPNs table displays the Fibre Channel address of the virtual port. When the physical Fibre Channel gateway port does not connect to storage, the address appears as 00:00:00.
AltBootupTargetWwpn	World-wide port name of the target that the initiator boots as an alternate.
AltBootupFcLunId	Identifier of the LU that contains the boot image that the initiator boots as an alternate.

Viewing Initiator-Target Connections with Storage Manager

To view initiator-target connections with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the SRP Hosts folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Click the initiator with connections to targets that you want to view, and then click the **Targets** tab.

The Targets Visible to This Host table appears in the right display. Table 13-6 describes the fields in this table.

Table 13-6 Targets Field Descriptions

Field	Description
Target WWPN	WWPNs of the target ports that the initiator sees.
Current Access	Fibre Channel gateway ports through which the initiator accesses the target storage port.
Physical Access	Fibre Channel gateway ports that physically connect the initiator to the target storage port.

Table 13-6 Targets Field Descriptions (continued)

Field	Description
Port Mask	Fibre Channel gateway ports (real and potential) that grant the initiator access to the target storage port.
Mode	Mode of the IT pair (**normal** or **test**).

Configuring the Mode of an Initiator-Target Pair

To configure the mode of an initiator-target pair, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Click the initiator with connections to targets that you want to view, and then click the **Targets** tab.

The Targets Visible to This Host table appears in the right pane.

Step 4 Click the entry of the IT pair that you want to configure, and then click **Edit**.

An IT Properties window opens.

Step 5 In the Mode field, click either the **Normal** or **Test** radio button.

Note The Current Access field must not contain any entries in order for you to configure the mode.

Viewing Initiator-LUN Connections with Storage Manager

To view initiator-LUN connections with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Click the initiator with connections to the LUNs that you want to view, and then click the **LUN Access** tab.

Table 13-7 describes the fields that appear in the right pane.

Table 13-7 LUN Access Field Descriptions

Field	Description
Available LUNs	Displays LUNs that the initiator has discovered but cannot currently access. Expand the **gateway** icon (), and then expand the **target** icon () to display the **LUN** icon (). **Note** When the initiator cannot communicate with the target or LUN, the icon appears gray instead of blue.
Accessible LUNs	Displays LUNs that the initiator currently accesses. Expand the **gateway** icon (), and then expand the **target** icon () to display the **LUN** icon ().

Discovering LUNs with Storage Manager

To discover the LUNs with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Click the initiator with connections to the LUNs that you want to view, and then click the **LUN Access** tab.

Step 4 Click **Discover LUNs**.

Deleting an Initiator with Storage Manager

To delete an initiator entry with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **SRP Hosts** folder.

Step 3 Select the initiator that you want to remove, and then click **Remove**.

Configuring Existing SRP Initiators with Storage Manager

To configure existing SRP initiators with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

A list of configured initiators appears beneath the SRP Hosts folder.

Step 3 Select the initiator that you want to configure, and then click the **General** tab.

Step 4 (Optional) In the Description field, edit the ASCII text description.

Step 5 (Optional) From the Boot Target WWPN drop-down menu, choose a boot target.

Step 6 (Optional) From the Boot Fibre Channel LUN drop-down menu, choose a boot LUN.

Step 7 Click **Apply**.

Viewing and Editing Initiator WWPNs

These topics describe how to view and edit initiator WWPNs:

- Viewing Initiator WWPNs, page 13-11
- Editing Virtual WWPNs, page 13-12

Viewing Initiator WWPNs

To view the initiator WWPNs that Fibre Channel gateway ports use to direct SAN traffic to SRP hosts, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Initiator WWPN** tab.

Table 13-8 describes the fields that appear in the display.

Table 13-8 Initiator WWPN Field Descriptions

Field	Description
Guid	Global unique identifier of the initiator.
Extension	GUID extension of the initiator.
Port	Physical Fibre Channel gateway port (real or potential).
Wwpn	Virtual world-wide port name that the physical Fibre Channel gateway port uses to direct SAN traffic to the initiator.
FcAddress	Fibre Channel address of the virtual port that directs SAN traffic to the SRP host.

Editing Virtual WWPNs

To edit a virtual WWPN, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Initiator WWPN** tab.

Step 3 In the Wwpn column, double-click the cell of the virtual WWPN that you want to edit and then change the value.

Note We strongly recommend that you never manually edit a virtual WWPN.

Step 4 Click **Apply**.

Viewing and Managing Target Ports

These topics describe how to view, edit, or add target ports:

Viewing Target Ports

To view the target ports that your Fibre Channel gateway has discovered, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Targets** tab.

Table 13-9 describes the fields that appear in the Targets table.

Table 13-9 Targets Table Field Descriptions

Field	Description
Wwpn	World-wide port name of the target storage port.
Description	ASCII text description of the target storage port. By default, the service name appears in this field.
IocGuid	Global unique identifier of the I/O controller (on the server switch) that manages the target.
ServiceName	Name of the Fibre Channel service.
ProtocolIds	Identifier of the Fibre Channel protocol.
FcAddress	Fibre Channel address of the target port.
Mtu	Maximum transmission unit of the target port.
PhysicalAccess	Physical Fibre Channel gateway ports that provide a path to the target port.
Wwnn	World-wide node name of the target storage device.
ConnectionType	All InfiniBand connections appear as Fibre Channel NL_Ports.

Editing SRP Targets

To edit SRP targets, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Targets** tab.

The Targets table appears.

Step 3 Identify the target that you want to edit and locate the appropriate entry in the table.

Step 4 (Optional) In the Description column, double-click the cell, and edit the ASCII description.

Step 5 (Optional) In the IocGuid column, double-click the cell, and edit the I/O controller GUID.

Note We strongly recommend that you do not manually edit the I/O controller GUID value.

Step 6 (Optional) In the ServiceName column, double-click the cell and edit the name of the service.

Step 7 Click **Apply**.

Adding SRP Targets

To manually add SRP targets, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Targets** tab.

The Targets table appears.

Step 3 Click **Insert**.

The Insert SRP Targets window appears.

Step 4 In the Wwpn field, enter the WWPN of the target.

Step 5 In the Description field, enter an ASCII text description of the target.

Step 6 In the IocGuid field, enter the GUID of the I/O controller for the target.

Step 7 In the ServiceName field, enter a service name for the target.

Step 8 Click **Insert**.

Step 9 Click **Apply**.

Viewing SRP Targets with Storage Manager

To view SRP targets with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Targets** folder.

The Targets Ports display appears. Table 13-10 describes the fields in the display.

Table 13-10 Targets Field Descriptions

Field	Description
Number of Active Targets	Number of active targets that connect to the server switch.
Number of Inactive Targets	Number of inactive targets that connect to the server switch.
Total Number of Targets	Number of targets that connect to the server switch.
WWPN	World-wide port name of the target port.

Table 13-10 Targets Field Descriptions (continued)

Field	Description
Description	ASCII text description of the target port.
Physical Access	Fibre Channel gateway ports that connect the server switch to the target port.

Editing SRP Targets with Storage Manager

To edit SRP target entries with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **Targets** folder.

A list of discovered targets appears below the folder.

Step 3 In the Targets folder, select the target that you want to edit.

Target details appear in the right pane of the display.

Step 4 (Optional) In the Description field, edit the ASCII description.

Step 5 (Optional) In the Service Name field, edit the service name.

Step 6 Click **Apply**.

Viewing and Editing Initiator-Target-LUN Groups

These topics describe how to view and edit initiator-target-LUN (ITL) groups:

- Viewing ITL Groups, page 13-15
- Editing ITLs, page 13-16

Viewing ITL Groups

To view ITLs, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **ITLs** tab.

Table 13-11 describes the fields that appear in the **ITLs** table.

Table 13-11 ITLs Table Field Descriptions

Field	Description
Guid	Global unique identifier of the initiator in the ITL.
Extension	GUID extension of the initiator in the ITL.
TargetWwpn	World-wide port name of the target port in the ITL.
FcLunId	Fibre Channel LUN identifier of the LUN in the ITL.
DeviceCategory	Type of storage device (random or sequential).
Description	Description of the ITL, in ASCII characters.
SrpLunId	Virtual LUN ID of the LUN in the ITL, used for LUN masking.
LogicalId	Identifier of the logical unit (LU) that the LUN in the ITL represents.
GatewayPortMaskPolicy	Physical Fibre Channel gateway ports that connect the initiator to the target and LUN.
LunPolicy	Displays restricted if the initiator does not have access to the LUN in the ITL and nonRestricted if the initiator accesses the LUN.
State	Ports through which an IT connection occurs.
PhysicalAccess	Ports through which the ITL is physically accessible.

Editing ITLs

To edit ITLs, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **ITLs** tab.

Step 3 Identify the ITL that you want to edit and locate the entry in the ITLs table.

Step 4 (Optional) In the Description cell, double-click the cell and edit the description.

Step 5 (Optional) In the SrpLunID column, double-click the cell and edit the LUN mask.

For details on LUN masking, see the *Cisco SFS 3000 Series Product Family Fibre Channel Gateway User Guide*.

Step 6 (Optional) In the LogicalId column, double-click the cell and edit the LU identifier.

Note We strongly recommend that you never manually edit the LogicalId field.

Step 7 (Optional) Edit the gateway port-mask policy as follows:

a. In the GatewayPortMaskPolicy column, double-click the cell.

The GatewayPortMaskPolicy window opens.

b. Check the check boxes of the ports that you want to add; uncheck the check boxes of the ports that you want to remove

c. Click **OK**.

Step 8 (Optional) In the LunPolicy column, click the cell and choose **restricted** or **nonRestricted** from the drop-down menu.

Step 9 Click **Apply**.

Viewing and Editing Initiator-Target Pairs

These topics describe how to view and edit initiator-target (IT) pairs:

Viewing ITs

To view IT pairs, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **ITs** tab.

Table 13-12 describes the fields that appear in the **ITs** table.

Table 13-12 IT Table Field Descriptions

Field	Description
Guid	Global unique identifier of the initiator in the IT pair.
Extension	GUID extension of the initiator in the IT pair.
TargetWwpn	World-wide port name of the target port in the IT pair.
Description	ASCII text description of the IT pair.
GatewayPortMaskPolicy	Fibre Channel gateway ports that let the initiator access the target.
State	Fibre Channel gateway ports that the IT pair currently uses.
PhysicalAccess	Fibre Channel gateway ports that create a physical connection between the target and the initiator.
Mode	Mode of the IT pair (normal or test).
Action	Last action that the IT pair took.
Result	Result of the last action that the IT pair took.

Editing ITs

To edit ITs, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **ITs** tab.

Step 3 Identify the IT that you want to edit and locate the entry in the ITs table.

Step 4 (Optional) In the Description cell, double-click the cell, and edit the description.

Step 5 (Optional) Edit the gateway port-mask policy as follows:

a. In the GatewayPortMaskPolicy column, double-click the cell.

The GatewayPortMaskPolicy window opens.

b. Check the check boxes of ports to add; uncheck the check boxes of the ports to remove.

c. Click **OK**.

Step 6 (Optional) In the Action column, click the cell and choose an action from the menu.

The action executes when you click **Apply**, and the result of the action appears in the Result column.

Step 7 Click **Apply**.

Viewing and Managing Logical Units

These topics describe how to view, edit, and add logical units (LUs):

Viewing LUs

To view the logical units that your Fibre Channel gateways have discovered, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **LUs** tab.

Table 13-13 describes the fields in the table.

Table 13-13 Logical Units Field Descriptions

Field	Description
LogicalId	ID of the LU.
DeviceCategory	Displays random or sequential to identify the type of LUN.
Description	User-defined LU description.
HiMark	Maximum number of outstanding requests from the initiator to the storage that the ITL can maintain.
MaxRetry	Number of failed communication attempts that must occur before the LUN identifies the initiator as inaccessible.
MinIoTimeout	Maximum amount of time that elapses before a SRP request times out.
DynamicPathAffinity	Displays true if you enable the feature and false if you disable the feature.
DynamicGatewayPortLoadBalancing	Displays true if you enable the feature and false if you disable the feature.
DynamicGatewayPortFailover	Displays true if you enable the feature and false if you disable the feature.
VendorId	Vendor-assigned ID of the LUN.
ProductId	Vendor-assigned product ID of the LUN.
ProductRevision	Manufacturer-assigned product revision number.
PhysicalAccess	Fibre Channel gateway ports on your server switch that connect to the LU.
Targets	Target port that provides access to the LU.
Size	Displays the size of the LUN in bytes.

Editing LU Entries

To edit LU entries, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **LUs** tab.

Step 3 Identify the LU entry that you want to edit and locate the entry in the **LUs** table.

Step 4 (Optional) In the DeviceCategory column, click the cell and choose **random** or **sequential** from the drop-down menu.

Step 5 (Optional) Double-click the cell in the Description field, and edit the ASCII text description of the LU.

Step 6 (Optional) Double-click the cell in the HiMark field, and edit the hi-mark value of the LU.

Step 7 (Optional) In the MaxRetry field, double-click the cell, and edit the maximum retry value of the LU.

Step 8 (Optional) In the DynamicPathAffinity column, click the cell, and choose true or false from the drop-down menu.

Step 9 (Optional) In the DynamicGatewayPortLoadBalancing column, click the cell, and from the drop-down menu, choose true or false.

Step 10 (Optional) In the DynamicGatewayPortFailover column, click the cell, and from the drop-down menu, choose true or false.

Step 11 (Optional) In the Targets column, double-click the cell, and edit the targets entry.

Note We strongly recommend that you do not edit the Targets field manually.

Step 12 Click **Apply**.

Manually Adding SRP LUs

To manually add SRP LUs, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **LUs** tab.

The LUs table appears.

Step 3 Click **Insert**.

The Insert SRP LUs window appears.

Step 4 In the LogicalId field, enter the LU ID of the LU.

Step 5 In the DeviceCategory field, click the **sequential** radio button for a tape device LU: otherwise, click the **random** radio button.

Step 6 In the Description field, enter a description.

Step 7 In the HiMark field, enter a high mark.

Step 8 In the MaxRetry field, enter a maximum retry value.

Step 9 In the MinIoTimeout field, enter a minimum timeout value.

Step 10 Check one of the following check boxes:

- DynamicPathAffinity
- DynamicGatewayPortLoadBalancing
- DynamicGatewayPortFailover

Step 11 In the Targets field, enter target WWPNs.

Step 12 Click **Insert**.

Step 13 Click **Apply**.

Viewing LUs with Storage Manager

To view LUs with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Logical Units** folder.

Table 13-14 describes the fields that appear.

Table 13-14 Logical Units Field Descriptions

Field	Description
Number of Active Logical Units	Number of active LUs that connect to the server switch.
Number of Inactive Logical Units	Number of inactive LUs that connect to the server switch.
Total Number of Logical Units	Number of LUs that connect to the server switch.
Logical Id	Logical ID of the LU.
Inquiry Data	Data received by the inquiry.
Physical Access	Fibre Channel gateway ports that connect the LUs to the server switch.

Editing LU Attributes with Storage Manager

To edit LU attributes with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **Logical Units** folder to display the LUs in the folder.

Step 3 Click a LU icon ( ) under the **Logical Units** folder.

Step 4 Click the **General** tab.

Step 5 (Optional) In the Description field, edit the ASCII text description.

Step 6 (Optional) In the Hi Mark field, enter an integer value.

Step 7 (Optional) In the Max Retry field, enter an integer value.

Step 8 (Optional) In the Min IO Timeout field, enter an integer value.

Step 9 (Optional) Click the **Path Affinity** radio button.

Step 10 Click **Apply**.

Editing Initiator Access to a LU

To edit initiator access to a LU, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **Logical Units** folder to display the LUs in the folder.

Step 3 Click an LU icon ( ) under the **Logical Units** folder.

Step 4 Click the **Initiator Access** tab.

The Available Hosts and Accessible Hosts fields appear.

Step 5 Expand all plus-sign (+) icons to reveal all available and accessible hosts.

Step 6 Add or remove accessible hosts as follows:

- In the Accessible Hosts field, select a host, and then click **Remove** to deny that host access to the LUN.
- In the Available Hosts field, select a host, and then click **Add** to grant that host access to the LUN.

Step 7 Click **Apply**.

Viewing and Graphing Global SRP Statistics

These topics describe how to view and graph global SRP statistics:

- Viewing Global SRP Statistics, page 13-22
- Viewing Global SRP Statistics with Storage Manager, page 13-23
- Graphing Global SRP Statistics with Storage Manager, page 13-24

Viewing Global SRP Statistics

To view global statistics, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Global Stats** tab.

Table 13-15 describes the fields that appear in the tab.

Table 13-15 Global Stats Field Descriptions

Field	Description
LinkEvents	Number of link events (for example, link up, link down) processed by the Fibre Channel interface gateway(s).
SrpInitiatedIos	Number of I/O transactions requested by the SRP initiator.

Table 13-15 Global Stats Field Descriptions (continued)

Field	Description
SrpCmdsCompleted	Number of SRP commands completed on the Fibre Channel interface gateway(s).
SrpBytesRead	Number of I/O bytes read by the SRP initiator that connects to this chassis.
SrpBytesWritten	Number of I/O bytes written by the SRP initiator.
SrpConnections	Number of connections used by the SRP initiator.
SrpCmdsOutstanding	Number of unresolved SRP commands on the Fibre Channel interface gateway(s).
SrpErrors	Number of SRP errors encountered on the Fibre Channel interface gateway(s).
FcpInitiatedIos	Number of I/O responses by the Fibre Channel device to SRP initiator requests.
FcpCmdsCompleted	Number of FCP commands completed on the Fibre Channel interface gateway(s).
FcpBytesRead	Number of I/O bytes read by the target device.
FcpBytesWritten	Number of I/O bytes written by the target device.
FcpCmdsOutstanding	Number of unresolved FCP commands on the Fibre Channel interface gateway(s).
FcpErrors	Number of FCP errors encountered on the Fibre Channel interface gateway(s).

Viewing Global SRP Statistics with Storage Manager

To view global SRP statistics with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 Click **Graph Global Statistics**.

The SRP Statistics window appears. Table 13-15 describes the fields in the rows of this window. Table 13-16 describes the fields in the columns of this window.

Note The elapsed time period appears in the bottom right of the SRP Statistics display.

Table 13-16 SRP Statistics Column Descriptions

Column	Description
AbsoluteValue	Cumulative value of the row since the server switch booted.
Cumulative	Cumulative value of the row over the elapsed time period.
Average	Average value of the row over the elapsed time period.
Minimum	Minimum value of the row over the elapsed time period.
Maximum	Maximum value of the row over the elapsed time period.
LastValue	Last change in the value of the row.

Step 4 (Optional) Click the drop-down menu at the bottom of the SRP Statistics window, and choose a refresh interval.

The data begins to refresh at the rate that you specify.

Graphing Global SRP Statistics with Storage Manager

To graph global SRP statistics, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 Click **Graph Global Statistics**.

The SRP Statistics window appears.

Step 4 Select the values that you want to include in the graph with one of the following methods:

- Click and drag your cursor across the values that you want to graph.
- Press the **Ctrl** key and select the values that you want to graph.

Step 5 Click the icon of the graph that you want to create. (See Figure 13-1.)

Figure 13-1 Graphing Icons

	**Line Chart**
	**Area Chart**
	**Bar Chart**
	**Pie Chart**

The graph appears. For different views of the data, see the "Swapping Chart Type, Layout, and Scale" section on page 13-25.

Note With most charts, the display will reload with updated information based on the refresh rate. To configure the interval, see the "Configuring Refresh Rate" section on page 13-26.

Swapping Chart Type, Layout, and Scale

With the exception of pie charts, the chart display lets you do the following:

- Swap between charts.
- Increase or decrease the scale of the display.
- View the chart horizontally or vertically.

Table 13-17 describes the icons used to complete these functions.

Table 13-17 Chart Icons

Icon	Function
	The Stacked icon overlays the graphical output of each statistic.
	The Horizontal icon rotates the axis of the graph by 90 degrees.
	The Log Scale icon zooms in and out.

Table 13-17 Chart Icons (continued)

Icon	Function
	The Line Chart icon displays a line chart.
	The Area Chart icon displays an area chart.
	The Bar Chart icon displays a bar chart.

Configuring Refresh Rate

Element Manager refreshes all statistics displays at regular intervals. To configure the refresh rate interval, follow these steps:

Step 1 In the chassis display, click a port with a refresh rate that you want to change.

Step 2 From the Report menu, choose **Graph Port**.

A window opens that displays the type and number of the port.

Step 3 Click the drop-down menu that appears at the bottom of the window, and choose the interval at which you want the display to refresh.

Note You do not need to click **Apply** or **OK**. The change takes place immediately.

Viewing and Graphing ITL Statistics

These topics describe how to view and graph ITL statistics:

- Viewing ITL Statistics, page 13-26
- Viewing ITL Statistics with Storage Manager, page 13-27
- Graphing ITL Statistics with Storage Manager, page 13-28

Viewing ITL Statistics

To view ITL statistics, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **ITL Stats** tab.

Table 13-18 describes the fields that appear in the tab.

Table 13-18 ITL Stats Field Descriptions

Field	Description
Guid	GUID of the initiator.
Extension	GUID extension of the initiator.
TargetWwpn	WWPN of the target.
FcLunId	LUN ID of the LUN in the ITL.
SlotId	Slot on the server switch in which the Fibre Channel gateway resides.
SrpInitiatedIos	Number of SRP I/O requests.
SrpCmdsCompleted	Cumulative number of commands that one or all Fibre Channel gateways executed.
SrpBytesRead	Cumulative number of SRP bytes read by one or all Fibre Channel gateways.
SrpBytesWritten	Cumulative number of SRP bytes written by one or all Fibre Channel gateways.
SrpCmdsOutstanding	Cumulative number of outstanding Fibre Channel commands.
SrpErrors	Cumulative number of SRP errors.
FcpInitiatedIos	Number of Fibre Channel I/O requests.
FcpCmdsCompleted	Cumulative number of commands that one or all Fibre Channel gateways executed.
FcpBytesRead	Cumulative number of Fibre Channel bytes read by one or all Fibre Channel gateways.
FcpBytesWritten	Cumulative number of Fibre Channel bytes written by one or all Fibre Channel gateways.
FcpCmdsOutstanding	Cumulative number of outstanding Fibre Channel commands.
FcpErrors	Cumulative number of Fibre Channel errors on one or all gateways.

Viewing ITL Statistics with Storage Manager

To view ITL statistics with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 From the Initiator drop-down menu, choose an initiator.

Step 4 From the Target drop-down menu, choose a target.

Step 5 From the LUN drop-down menu, choose a logical unit.

Step 6 From the Gateway drop-down menu, choose a Fibre Channel gateway.

Step 7 Click **Graph ITL Statistics**.

The ITL Statistics window opens. Table 13-18 describes the fields in this window. Table 13-19 describes the columns in this window.

Table 13-19 SRP Statistics Column Descriptions

Column	Description
AbsoluteValue	Cumulative value of the row since the server switch booted.
Cumulative	Cumulative value of the row over the elapsed time period.
Average	Average value of the row over the elapsed time period.
Minimum	Minimum value of the row over the elapsed time period.
Maximum	Maximum value of the row over the elapsed time period.
LastValue	Last change in the value of the row.

Graphing ITL Statistics with Storage Manager

To graph ITL statistics with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 From the Initiator drop-down menu, choose an initiator.

Step 4 From the Target drop-down menu, choose a target.

Step 5 From the LUN drop-down menu, choose a logical unit.

Step 6 From the Gateway drop-down menu, choose a Fibre Channel gateway.

Step 7 Click **Graph ITL Statistics**.

The ITL Statistics window opens.

Step 8 Select the values that you want to include in the graph with one of the following methods:

- Click and drag your cursor across the values that you want to graph.
- Press the **Ctrl** key and select the values that you want to graph.

Step 9 Click the icon of the graph (see Figure 13-2) that you want to create.

Figure 13-2 Graphing Icons

	**Line Chart**
	**Area Chart**
	**Bar Chart**
	**Pie Chart**

The graph appears. For different views of the data, see the "Swapping Chart Type, Layout, and Scale" section on page 13-29.

Note With most charts, the display will reload with updated information based on the refresh rate. To configure the interval, see the "Configuring Refresh Rate" section on page 13-26.

Swapping Chart Type, Layout, and Scale

With the exception of pie charts, the chart display lets you do the following:

- Swap between charts.
- Increase or decrease the scale of the display.
- View the chart horizontally or vertically.

Table 13-20 describes the icons used to complete these functions.

Table 13-20 Chart Icons

Icon	Function
	The Stacked icon overlays the graphical output of each statistic.
	The Horizontal icon rotates the axis of the graph by ninety degrees.
	The Log Scale icon zooms in and out.
	The Line Chart icon displays a line chart.

Table 13-20 Chart Icons (continued)

Icon	Function
	The Area Chart icon displays an area chart.
	The Bar Chart icon displays a bar chart.

Viewing and Graphing Gateway Statistics

These topics describe how to view and graph gateway statistics:

- Viewing Gateway Statistics, page 13-30
- Viewing Gateway Statistics with Storage Manager, page 13-31
- Graphing Gateway Statistics with Storage Manager, page 13-32

Viewing Gateway Statistics

To view Fibre Channel gateway statistics, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

Step 2 The SRP window opens.

Step 3 Click the **Gateway Stats** tab.

Table 13-21 describes the fields that appear in the tab.

Table 13-21 Gateway Stats Field Descriptions

Field	Description
SlotId	Slot in the server switch in which the Fibre Channel gateway resides.
LinkEvents	Number of link events (for example, link up, link down) processed by the Fibre Channel interface gateway(s).
SrpCmdsOutstanding	Number of incomplete SRP commands on the Fibre Channel interface gateway(s).
SrpCmdsCompleted	Number of SRP commands completed on the Fibre Channel interface gateway(s).
SrpErrors	Number of SRP errors encountered on the Fibre Channel interface gateway(s).
SrpInitiatedIos	Number of I/O transactions requested by the SRP initiator.
FcpCmdsOutstanding	Number of incomplete FCP commands on the Fibre Channel interface gateway(s).
FcpCmdsCompleted	Number of FCP commands completed on the Fibre Channel interface gateway(s).

Table 13-21 Gateway Stats Field Descriptions (continued)

Field	Description
FcpErrors	Number of FCP errors encountered on the Fibre Channel interface gateway(s).
FcpInitiatedIos	Number of I/O responses by the Fibre Channel device to SRP initiator requests.
SrpBytesRead	Number of I/O bytes read by the SRP initiator that connects to this chassis.
SrpBytesWritten	Number of I/O bytes written by the SRP initiator.
FcpBytesRead	Number of I/O bytes read by the target device.
FcpBytesWritten	Number of I/O bytes written by the target device.
SrpConnections	Number of connections used by the SRP initiator.

Viewing Gateway Statistics with Storage Manager

To view gateway statistics with Storage Manager, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 In the Gateways field, select a gateway with statistics that you want to view.

Step 4 Click **Graph Gateway Statistics**.

Step 5 The SRP Statistics window appears.

Table 13-21 describes the fields in the rows of this window. Table 13-22 describes the fields in the columns of this window.

Note The elapsed time period appears in the bottom right of the SRP Statistics display.

Table 13-22 SRP Statistics Column Descriptions

Column	Description
AbsoluteValue	Cumulative value of the row since the server switch booted.
Cumulative	Cumulative value of the row over the elapsed time period.
Average	Average value of the row over the elapsed time period.
Minimum	Minimum value of the row over the elapsed time period.
Maximum	Maximum value of the row over the elapsed time period.
LastValue	Last change in the value of the row.

Step 6 (Optional) Click the drop-down menu at the bottom of the SRP Statistics window, and choose a refresh interval.

The data begins to refresh at the rate that you specify.

Graphing Gateway Statistics with Storage Manager

To graph gateway SRP statistics, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Statistics** folder.

Statistics fields appear in the right pane of the display.

Step 3 In the Gateways field, select the gateway with statistics that you want to view.

Step 4 Click **Graph Gateway Statistics**.

The SRP Statistics window appears.

Step 5 Select the values that you want to include in the graph with one of the following methods:

- Click-and-drag your cursor across the values that you want to graph.
- Press the **Ctrl** key and select the values that you want to graph.

Step 6 Click the icon of the graph (see Figure 13-3) that you want to create.

Figure 13-3 Graphing Icons

	**Line Chart**
	**Area Chart**
	**Bar Chart**
	**Pie Chart**

The graph appears. For different views of the data, see the "Swapping Chart Type, Layout, and Scale" section on page 13-33.

Note With most charts, the display will reload with updated information based on the refresh rate. To configure the interval, see the "Configuring Refresh Rate" section on page 13-26.

Swapping Chart Type, Layout, and Scale

With the exception of pie charts, the chart display lets you do the following:

- Swap between charts.
- Increase or decrease the scale of the display.
- View the chart horizontally or vertically.

Table 13-23 describes the icons used to complete these functions.

Table 13-23 Chart Icons

Icon	Function
	The Stacked icon overlays the graphical output of each statistic.
	The Horizontal icon rotates the axis of the graph by ninety degrees.
	The Log Scale icon zooms in and out.
	The Line Chart icon displays a line chart.
	The Area Chart icon displays an area chart.
	The Bar Chart icon displays a bar chart.

Viewing Recommended World Wide Names

To view recommended world-wide node names and world-wide port names, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **WWN Allocator** tab.

Step 3 In the Guid field, enter the GUID of the initiator for which you want to procure a WWNN or WWPN.

Step 4 In the Extension field, enter the GUID extension of the initiator for which you want to procure a WWNN or WWPN.

Step 5 in the Port field, click the **...** button, and select a port for which you want to procure a WWPN.

Step 6 Click the **getRecommendedWwnn** radio button, and then click **Apply** to display the recommended WWNN in the RecommendedWwnn field.

Step 7 Click the **getRecommendedWwpn** radio button, and then click **Apply** to display the recommended WWPN in the RecommendedWwpn field.

Disconnecting ITLs on a Fibre Channel Gateway

To disconnect all ITLs through a particular Fibre Channel gateway, follow these steps:

Step 1 From the FibreChannel menu, choose **SRP**.

The SRP window opens.

Step 2 Click the **Action** tab.

Step 3 Click the **disconnectAllItls** radio button.

Step 4 In the SlotId field, enter the slot of the Fibre Channel gateway with ITLs that you want to disconnect.

Step 5 Click **Apply**.

Viewing Fibre Channel Gateways on the server switch

These topics describe how to view Fibre Channel gateways on the server switch:

- Viewing All Fibre Channel Gateways, page 13-34
- Viewing Individual Fibre Channel Gateways, page 13-35
- Redistributing Connections Over a Gateway, page 13-35

Viewing All Fibre Channel Gateways

To view the all Fibre Channel gateways on your server switch, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **Gateway Cards** folder.

The Gateway Cards display appears in the right pane of the window. Table 13-24 describes the fields in this pane.

Table 13-24 Gateway Cards Field Descriptions Pane

Field	Description
Gateway	Lists the gateways that reside in the server switch.
Initiator-Target Connections	Displays the number of IT connections that connect through the gateway.
ITLs	Displays the number of ITL connections that connect through the gateway.

Viewing Individual Fibre Channel Gateways

To view an individual Fibre Channel gateway, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

Step 2 The Storage Manager window opens.

Step 3 Expand the **Gateway Cards** folder.

Step 4 Select a gateway below the **Gateway Cards** folder.

The Active ITLs display appears.

Step 5 In the Active ITLs display, expand an initiator to list the targets available to the initiator.

Step 6 In the Active ITLs display, expand a target to list the LUs available to the initiator through that target.

Redistributing Connections Over a Gateway

To redistribute connections over a gateway, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

Step 2 The Storage Manager window opens.

Step 3 Expand the **Gateway Cards** folder.

Step 4 Select a gateway below the **Gateway Cards** folder.

Step 5 Click **Redistribute Connections**.

Viewing and Managing SRP Hosts

These topics describe how to view and manage SRP hosts:

Viewing SRP Hosts

To view SRP hosts, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **SRP Hosts** folder.

Table 13-25 describes the fields that appear in the display.

Table 13-25 SRP Hosts Field Descriptions

Field	Description
Number of Active Hosts	Number of active hosts that connect to the server switch.
Number of Inactive Hosts	Number of inactive hosts that connect to the server switch.
Total Number of Hosts	Number of hosts that connect to the server switch.
Host	ASCII text name of the host.
WWNN	World-wide node name of the host.
Ports Registered With	Fibre Channel gateway ports that connect the hosts to storage.

Defining a New SRP Host

To define a new SRP host, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

Step 2 The Storage Manager window opens.

Step 3 Select the **SRP Hosts** folder.

Step 4 Click **Define New**.

The Define New SRP Host window appears.

Step 5 Enter the GUID of your host in the Host GUID field, or choose it from the drop-down menu.

Note If your host successfully connects to your server switch, the GUID appears in the drop-down menu. To create a SRP host entry for a host not yet connected, manually enter the digits of the GUID in the field. Element manager automatically enters colons (:) as you enter digits.

Step 6 (Optional) In the Description field, enter an ASCII text description of the host.

Step 7 Click **Next**.

The WWNN and WWPNs of the entry appear.

Step 8 Click **Finish**.

Deleting SRP Hosts

To delete an SRP host, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Select the **SRP Hosts** folder.

Step 3 Select the SRP host that you want to delete, and then click **Remove**.

Granting or Denying SRP Host Target Access

To grant or deny the initiator access to SRP host targets, follow these steps:

Step 1 From the FibreChannel menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

Step 3 Select the host with the target access that you want to edit.

Step 4 Click the **Targets** tab.

Step 5 Double-click the target entry to which you want to grant or deny the initiator access.

The IT Properties window opens.

Step 6 Click the **...** button next to the Port Mask field.

The Select Port(s) window opens.

Step 7 Check the check boxes of the ports through which you want to grant the initiator access to the target; uncheck the check boxes through which you want to deny the initiator access to the target.

Step 8 Click **Ok**, and then click **Apply**.

Editing SRP Hosts LUN Access

To edit a a LUN access of an SRP host, follow these steps:

Step 1 From the **FibreChannel** menu, choose **Storage Manager**.

The Storage Manager window opens.

Step 2 Expand the **SRP Hosts** folder.

Step 3 Select the host with target access that you want to edit.

Step 4 Click the **LUN Access** tab.

Step 5 Add or remove accessible LUNs as follows:

- Select a host in the Accessible LUNs field, and then click **Remove** to deny that host access to the LUN.
- Select a host in the Available LUNs field, and then click **Add** to grant that host access to the LUN.

CHAPTER 14

Help Menu Tasks

These topics describe the Help menu tasks of Element Manager:

Note The tasks under the Help menu provide Element Manager resources and Support resources. For context-sensitive online help, click the **Help** button in any Element Manager window.

Launching Online Help

To launch the online help, choose **Contents** from the Help menu. Element Manager online help launches.

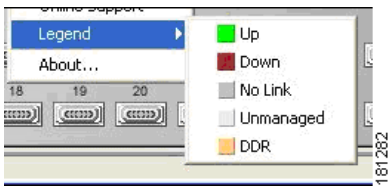
Launching the Support Website

To launch the support Web site, choose **Online Support** from the Help menu. The support website launches.

Viewing the Element Manager Status Legend

To view the Element Manager status legend, choose **Legend** from the Help menu. The Element Manager legend appears.

Figure 14-1 Element Manager Help



APPENDIX A

InfiniBand Concepts

These topics describe InfiniBand concepts:

Understanding InfiniBand

InfiniBand is a high speed, high density serial interconnect that increases CPU utilization, decreases latency, and eases the management problems of data centers. The term “InfiniBand” refers to the entire hardware, communication, and management infrastructure. Use of this technology increases the communication speed between the following:

- CPUs
- Devices within servers
- Subsystems located throughout a network

InfiniBand combines high-speed hardware, specialized protocols, and Remote Data Memory Access (RDMA) techniques to increase CPU utilization and decrease latency. Operations of the InfiniBand Architecture are managed by the Subnet Manager.

These topics provide further details:

InfiniBand Components

One or more of the following hardware components may be used to maximize your server network:

- InfiniBand switch—Passes traffic between InfiniBand-capable devices over the InfiniBand network
- Host channel adapters (installed in host)—Serves as an InfiniBand version of a network interface card (NIC) to connect the host to the InfiniBand network

- Ethernet gateway—Provides Ethernet connectivity to an InfiniBand network
- Fibre Channel gateway—Provides Fibre Channel connectivity to an InfiniBand network

Protocols

InfiniBand requires a new set of protocols. All of the necessary protocol drivers are included with the server switch. These protocols include:

- IPoIB, page A-2
- SDP, page A-2
- SRP, page A-2
- uDAPL, page A-2

IPoIB

The IP over InfiniBand (IPoIB) link driver provides standardized IP encapsulation over InfiniBand fabrics. IPoIB can transparently use IP over InfiniBand technology, which is similar to the way that IP runs over Ethernet.

You can use the IPoIB driver to perform an address resolution and manage the multicast membership.

SDP

The Sockets Direct Protocol (SDP) is a transparent protocol used on InfiniBand networks to allow sockets-based applications to take advantage of the RDMA performance over an InfiniBand network. SDP reduces the amount of software running inside a process context. The zero-copy SDP support enables databases, application servers, and CPUs to operate more efficiently because the databases spend less time waiting for work, the application servers spend less time waiting for responses, and the CPUs have more cycles free for other work.

SRP

The SCSI RDMA Protocol (SRP) is an upper-layer storage protocol for InfiniBand that runs SCSI commands across RDMA-capable networks for InfiniBand hosts to communicate with Fibre Channel storage devices. This protocol allows InfiniBand hosts to natively send SCSI commands as if the storage was directly attached.

The SRP protocol uses an RDMA communication service that provides communication between pairs of consumers; it uses messages for control information and RDMA operations for data transfers.

The SRP protocol is used only if you have a Fibre Channel Gateway installed in your InfiniBand system.

uDAPL

The user Direct Access Programming Library (uDAPL) is a standardized user mode API that natively supports InfiniBand fabrics. uDAPL performs name-to-address translations, establishes connections, and transfers data reliably. The primary responsibilities of uDAPL are connection management and low latency data transfer and completion.

Architectural Elements

The following structures serve as foundational elements of InfiniBand architecture:

- RDMA, page A-3
- Queue Pairs, page A-3

RDMA

InfiniBand uses RDMA technology. RDMA allows one computer to place information directly into the memory of another computer. RDMA allows user space applications to directly access hardware and zero-copy data movement.

A combination of hardware and software allows user space applications to read and write the memory of a remote system without kernel intervention or unnecessary data copies. This feature results in lower CPU utilization per I/O operation and more efficient use of machine resources because applications place most of the messaging burden upon the InfiniBand high-speed network hardware.

Queue Pairs

The queue pair (QP) is one of the primary architectural elements of InfiniBand. In InfiniBand, communication occurs between queue pairs, instead of between ports.

A queue pair is an addressable entity that consists of two work queues: a Send work queue and a Receive work queue. The Channel Adapter hardware arbitrates communication by multiplexing access to the send queue or demultiplexing messages on the receive queue.

Note A verb is used to define the functionality of the Host Channel Adapter (HCA). A "verb consumer" refers to the direct user of the verb.

A work queue provides a consumer with the ability to queue up a set of instructions that are executed by the Channel Adapter. There are two types of work queues: Send work queues (outbound) and a receive work queues (inbound). Together these work queues create a queue pair.

A connection is made by linking a local queue pair to a remote queue pair. Applications do not share queue pairs; once you set them up, you can manage them at the application level without incurring the overhead of system calls.

Send and receive work queues have these characteristics:

- Always created as a pair.
- Always remain a pair.
- Known as QPs.
- Identified by a queue pair number, which is within the Channel Adapter.

Queue pairs have these characteristics:

- A region of memory to be used as buffers (numbers of queue pairs are only limited by memory).
- A key that must match on each incoming packet (the Q_Key) to verify the validity of the packet.
- (Potentially) a partition key, which specifies the portion of the fabric that this queue pair may access.

The queue pair is the mechanism by which you define quality of service, system protection, error detection and response, and allowable services.

Each queue pair is independently configured for a particular type of service. These service types provide different levels of service and different error-recovery characteristics as follows:

- Reliable connection
- Unreliable connection
- Reliable datagram
- Unreliable datagram

Once the fabric connections are discovered, queue pairs and protection domains are established, the type and quality of service are defined for each queue pair, and the fabric operates reliably and securely at full QoS without impacting system hardware or software resources.

Understanding the Subnet Manager

The Subnet Manager configures and maintains fabric operations. There can be multiple Subnet Managers but only one master. The Subnet Manager is the central repository of all information that is required to set up and bring up the InfiniBand fabric.

The master Subnet Manager does the following:

- Discovers the fabric topology.
- Discovers end nodes.
- Configures switches and end nodes with their parameters, such as the following:
  - Local Identifiers (LIDs)
  - Global Unique Identifier (GUIDs)
  - Partition Key (P_Keys)
- Configures switch forwarding tables.
- Receives traps from Subnet Management Agents (SMAs).
- Sweeps the subnet, discovering topology changes and managing changes as nodes are added and deleted.

These topics provide additional details:

- Subnet Management Agents, page A-4
- Subnet Manager Hot Standby, page A-4

Subnet Management Agents

Subnet Manager Agents are part of the Subnet Manager. A Subnet Manager Agent is provided with each node and processes packets from the Subnet Manager.

If a Subnet Manager is elected master, all of its components, including Subnet Agent, are implicitly elected master. If a Subnet Manager ceases to be the master, all of its components cease responding to messages from clients.

Subnet Manager Hot Standby

The master and slave Subnet Managers can be synchronized so that the information in the master is carried over to the slave if a failover occurs. See the "Enabling Subnet Manager Database Synchronization" section on page 8-12 to configure the hot-standby Subnet Manager.

The hot standby/database synchronization feature is used to synchronize the databases between Subnet Managers running on separate chassis.

The Subnet Manager maintains a database in the volatile memory of the master Subnet Manager. Database synchronization is accomplished in two stages:

- Cold Synchronization—This stage is initiated by the master Subnet Manager when it is ready to start a synchronization session with a standby Subnet Manager. In this stage, tables that are not synchronized are copied from the master Subnet Manager to the standby Subnet Manager.
- Transactional Synchronization—This stage is entered following the successful completion of the cold synchronization stage. In this stage, all database update transaction requests that are processed by the master, are replicated to the standby Subnet Manager.

A standby Subnet Manager can become the master in any of these situations:

- The node that is running the current master Subnet Manager crashes.
- Partitioning of the subnet (such as due to a link failure) takes place.
- Graceful shutdown of the master (such as for maintenance purposes) takes place.

The following occurs in the event of a failure:

- The standby Subnet Manager becomes the new master.
- The new master rebuilds the database from information retrieved during the subnet discovery phase.
- Existing LID assignments are retained, where possible.
- All ports are reset to force them to rejoin multicast groups, advertise the services again, request event forwarding again, and reestablish connections.
- A SlaveToMaster event trap is generated to trigger any necessary processing by external management applications.

Subnet Manager Routing

There are two different concepts associated with InfiniBand routing:

- Routing internally within a switch (hops between switch chips)
- Routing between whole switches (hops between nodes)

Note This process is also referred to as routing between switch elements.

Internal switch routing can be configured to provide the highest performance in passing traffic and to minimize the threat of congestion within the switch.

The routing process is as follows:

Step 1 The Subnet Manager discovers all the InfiniBand switch chips in the network.

Step 2 The Subnet Manager groups the internal switch chips within each chassis into a switch element.

Step 3 The Subnet Manager process continues until all the InfiniBand switches are grouped into switch elements.

Step 4 After all the switch chips are grouped, the Subnet Manager routes the switch elements according to the routing algorithm discussed in the "Minimum Contention, Shortest Path, and Load Balancing Algorithm" section on page A-6.

Step 5 The internal network of each InfiniBand switch is then routed based on the best algorithm for each switch element.

These topics provide additional details:

Multiple Paths

The Subnet Manager allows you to define the Local Identifier Mask Control (LMC) value per subnet. The default value of the LMC is 0. By default, only one Local Identifier (LID) is assigned to each host port.

Once the LMC value has been assigned, the Subnet Manager will route different paths for each LID associated with the same host port. The result of these paths is based on the applied routing algorithm.

Understanding Subnet Manager Routing Terms

The following terms are important to understand before distinguishing the various types of algorithms that the Subnet Manager uses for routing:

- Tolerance is used when deciding if a particular path is better in distance than the already selected path. You can choose the tolerance to be used for the shortest path calculation as follows:
  - If the tolerance is set to 0, a pair of distinct paths to an endport are said to be of equal distance if the number of hops in the paths is the same.
  - If the tolerance is set to 1, a pair of distinct paths to an endport are said to be of equal distance if the difference in their hop count is less than or equal to one.
- Contention is declared for every switch port on the path that is already used for routing another LID associated with the same host port.

Minimum Contention, Shortest Path, and Load Balancing Algorithm

The Minimum Contention, Shortest Path, and Load Balancing algorithm is used by default to route between the switch elements and between the internal InfiniBand switch chips within each switch element.

The following process shows how the algorithm makes the calculation:

Step 1 The shortest path for each of the host ports is calculated.

Step 2 Contention is calculated for all the available paths that are within the (shortest path + tolerance) distance.

a. The path with the least contention is selected.

b. If two paths have the same contention, the path with less distance is selected.

c. If two paths have the same contention and the same distance, the port usage count is used to provide load balancing over the two paths. The usage count is a measure of how many LIDs have been configured to use that particular port.

Deterministic Source-Based Routing Algorithm

The Deterministic Source Based Routing algorithm is used in some high-performance computing environments where the requirements may need to be more stringently defined. An administrator can identify the exact route that a given port and LID takes for traversing through the network.

Currently, only the internal routing for the Cisco SFS 7008 (a 96-port switch) supports this routing scheme. See the Cisco SFS 7008 Hardware Guide, or contact Cisco TAC for more information.

Configuring Your Network For Optimal Routing

For optimal routing, we recommend that you follow these steps:

- Create equal paths between switch elements
- Determine the first path that will be discovered

We recommend that InfiniBand switch elements be connected so that all paths between any pair of switch elements are the same distance (same number of hops), if possible. This process enables you to obtain the optimal paths using the default tolerance of 0. If the paths have different lengths, then the tolerance value will need to be determined.

The Subnet Manager Routing Algorithm selects the first best path that it finds. If multiple paths with the same properties are available, then the first of these paths found is the one that is selected. It is possible to set up the cabling between switch elements to force the algorithm to prioritize certain paths. Depending on the network requirements, the prioritized paths can either be concentrated on a particular switch element or spread across multiple switch elements to improve fault tolerance.

Understanding Partitions

A partition defines a set of InfiniBand nodes that are permitted to communicate with one another. Partitions do the following:

- Increase security.
- Divide a large cluster into small isolated subclusters.
- Map InfiniBand nodes to selected VLANs.

Note If db-sync is enabled, changes to partition configuration are allowed only on the chassis running the master subnet manager. For more information, see the "Configuring Database Synchronization" section on page 8-11.

These topics provide details:

How Partitions Work

A partition defines a set of InfiniBand nodes that are permitted to communicate with one another. Each node may be part of multiple partitions so that a system administrator can define overlapping partitions as the situation requires. Normal data packets carry a 16-bit P_Key, or partition key, that defines a unique partition. The Subnet Manager configures the channel adaptor for each node with its set of P_Keys. When a packet arrives at a node, the channel adapter checks that the packet's P_Key is valid based on the Subnet Manager's configuration. Packets with invalid P_Keys are discarded. P_Key validation prevents a server from communicating with another server outside of its partition.

InfiniBand partitions are comparable to hardware-enforced security features of conventional I/O networking technologies, such as Ethernet VLANs and Fibre-Channel zones.

Partition Members

Without members, a partition does not have meaning to the system. Ports are added to the partition and become members of that partition. Each port may be part of multiple partitions so that you can define overlapping partitions as the situation requires.

At the time a port member is added to the partition, you must decide whether that particular port will have full or limited membership.

Membership Types

A partition contains a group of members, but different types of members can exist within a single partition. Partition membership allows even further control because it defines communication within the members of that group, not just outside of it.

There are two types of partition memberships: full membership and limited membership. A full-membership partition member can communicate with all other partition members including other full members and limited members. A limited-membership partition member cannot communicate with other limited-membership partition members. However, a limited partition member can communicate with a full member.

About the Default Partition

The Subnet Manager automatically configures a default partition, which is always p_key ff:ff.

The default partition controls all connected ports, and by default, everything is a full member of the default partition. The default p_key cannot be altered or deleted as it is the controlling mechanism that manages the configuration of all the partitions.

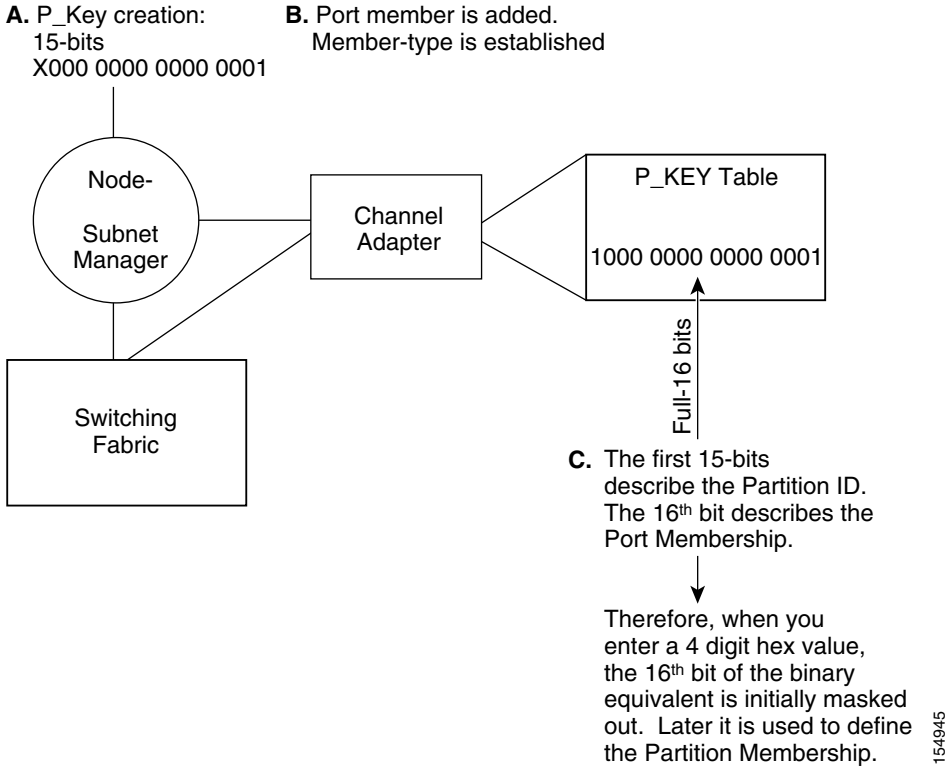
Selecting a P_Key Value

For a list of acceptable P_Key values, see Table A-2 on page A-10.

Upon creation, the p_key value (see Figure A-1) is technically a 15-bit number. However, after the p_key is created and the port(s) membership type has been established, the entire value becomes 16 bits. The most significant bit (MSB) displays the type of membership (0 = Limited member, 1 = Full member).

When assigning a p_key value, you need to choose four hexadecimal numbers. However, because of the way that the 16th bit is used, only certain numbers can be used for the most significant digit. Do not attempt to create two P_Keys differing only in the most significant bit of their 16-bit numbers. The system views them as the same P-Key. For example, 0 #:# # is the same P-Key as 8#:# #.

Figure A-1 Partition Keys



These topics provide further help in selecting a P_Key value:

- Hexadecimal to Binary Conversions, page A-10
- Examples of Valid P_Key Values, page A-10

Hexadecimal to Binary Conversions

Table A-1 is provided to assist in the creation of P_keys. When creating the partition p_key, enter a hexadecimal value that is the equivalent of 16 bits in binary. For example, enter 80:00 (hex) to be 1000000000000000 (binary). The default partition (which cannot be altered) is 7f:ff.

Table A-1 Binary Conversions

Hexadecimal	Binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Examples of Valid P_Key Values

You can choose your own p_key values, or you can choose your values from the list in Table A-2.

Table A-2 Valid P_Key Numbers

00:01	00:11
00:02	00:12
00:03	00:13
00:04	00:14
00:05	00:15
00:06	00:16
00:07	00:17
00:08	00:18
00:09	00:19
00:10	00:20

Understanding how P_Keys are Saved

Partition information is saved by the master Subnet Manager. If db-sync is enabled, the master Subnet Manager synchronizes P_key information to standby Subnet Managers (currently, only one standby manager is allowed). A synchronized standby retains the information from the master.

If you configure only one InfiniBand switch, it is automatically the master, and the partition configuration is saved persistently on the switch. See the "Enabling Subnet Manager Database Synchronization" section on page 8-12 for details.

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W