Cisco SFS Product Family Chassis 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-9162-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco SFS Product Family Chassis Manager User Guide
© 2006-2007 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Audience ix

Organization ix

Conventions x

Related Documentation xi

Obtaining Documentation, Obtaining Support, and Security Guidelines xi

CHAPTER 1 **About Chassis Manager** 1-1

Introduction 1-1

System Frame 1-1

Tree Frame 1-2

View Frame 1-6

Browser Requirements 1-7

Platform Requirements 1-8

CHAPTER 2 **Getting Started** 2-1

Preparing Your Device 2-1

Configuring an IP Address for a Cisco SFS 7000D Server Switch Using DHCP 2-2

Configuring a Static IP Address 2-2

Configuring an IP Address Dynamically on a Device for which DHCP is not the Default 2-3

Enabling HTTP or HTTPS Services 2-4

Launching Chassis Manager 2-4

Launching Chassis Manager without SSL 2-4

Launching Chassis Manager with SSL 2-5

Netscape/Mozilla 2-5

Internet Explorer 2-5

Avoiding Error Messages 2-7

Logging Out of Chassis Manager 2-8

Navigating Chassis Manager 2-8

Moving Backward 2-9

Refreshing Views 2-9

Understanding Access Privileges 2-9

Viewing the Device Status 2-9

CHAPTER 3 **Chassis Tasks 3-1**

Viewing Cards on a Chassis 3-1
Viewing Card Summary Information 3-1
Viewing Card Properties 3-3
Viewing the Card Inventory 3-6
Configuring the Administrative Status of a Card 3-7
Viewing Internal Gateway Ports 3-7
Viewing Physical Ports on a Chassis 3-8
Viewing All Ports 3-8
Viewing Port Properties 3-8
Viewing Port Bridging Properties 3-11
Viewing Port Statistics 3-11
Configuring Ports 3-13
Configuring a Port Name 3-13
Enabling or Disabling a Port 3-13
Configuring Autonegotiation on a Port 3-14
Configuring Port Speed 3-14
Clearing InfiniBand Port Counters 3-15
Viewing Power Supply Status 3-15
Viewing Power Supply Summary Information 3-15
Viewing Power Supply Properties 3-16
Viewing Fan Status 3-17
Viewing Fan Summary Information 3-17
Viewing Fan Properties 3-17
Viewing Temperature Sensor Status 3-18
Viewing the Backplane Information 3-19
Viewing Management Ports on a Chassis 3-19
Setting the Partition for the InfiniBand Management Port 3-21

CHAPTER 4 **Maintenance Tasks 4-1**

Configuring Basic System Information 4-1
Viewing System Information 4-2
Naming Your InfiniBand Switch 4-2
Defining a Device Location 4-3
Defining a Cisco TAC Resource 4-3
Configuring System Global Settings 4-3

Configuring System Operation Mode 4-3
Enabling or Disabling InfiniBand Counter Reset 4-4
Configuring Date and Time Properties 4-4
Configuring the Date and Time 4-4
Assigning NTP Servers 4-5
Configuring the Local Time Zone and Daylight Savings Time 4-5
Setting a Time Zone and Daylight Savings Time 4-5
Resetting the Time Zone and Daylight Savings Time 4-6
Viewing or Deleting Files in the File System 4-6
Viewing Files in the File System 4-7
Deleting Files in the File System 4-7
Installing Software Images 4-8
Importing Configuration Files and Image Files with FTP or SCP 4-8
Exporting Configuration Files and Log Files with FTP or SCP 4-9
Customizing the Boot Configuration 4-9
Deleting or Overwriting the Startup Configuration 4-10
Backing Up the Running Configuration File 4-10
Saving a Configuration File 4-11
Rebooting the Device 4-11
Configuring Basic Services 4-11
Assigning a DNS Server 4-12
Enabling or Disabling the FTP Access 4-12
Enabling or Disabling the Telnet Access 4-12
Assigning a Syslog Server 4-13
Assigning an Authentication Method 4-13
Configuring HTTP and HTTPS 4-15
Viewing and Managing RADIUS Servers 4-15
Viewing RADIUS Servers 4-15
Viewing and Configuring RADIUS Server Properties 4-16
Adding RADIUS Servers 4-17
Deleting RADIUS Servers 4-18
Viewing and Managing TACACS Servers 4-18
Viewing TACACS Servers 4-18
Viewing and Configuring TACACS Server Properties 4-19
Adding TACACS Servers 4-20
Deleting TACACS Servers 4-21
Viewing Authentication Failures 4-21
Viewing Diagnostic Test Results 4-22

Viewing Card POST Test Results 4-22
Viewing Fan POST Test Results 4-23
Viewing Power Supply POST Test Results 4-23
Viewing Card FRU Errors 4-24
Viewing Fan FRU Errors 4-24
Viewing Power Supply FRU Errors 4-25

CHAPTER 5 InfiniBand Tasks 5-1

Viewing and Managing Subnet Managers 5-1
Viewing Subnet Managers 5-1
Viewing Subnet Manager Properties 5-2
Adding a Subnet Manager 5-4
Deleting a Subnet Manager 5-4
Configuring Subnet Manager Properties 5-4
Viewing InfiniBand Services 5-6
Viewing InfiniBand Services Summary Information 5-6
Viewing InfiniBand Service Properties 5-6
Viewing InfiniBand Nodes 5-7
Viewing InfiniBand Node Summary Information 5-7
Viewing Node Properties 5-8
Viewing Node Ports 5-10
Viewing Node Neighbors 5-10
Viewing InfiniBand Ports 5-10
Viewing All InfiniBand Ports 5-11
Viewing InfiniBand Port Properties 5-11
Viewing Neighboring InfiniBand Devices 5-16
Viewing All Neighboring InfiniBand Devices 5-16
Viewing InfiniBand Neighbor Properties 5-17
Viewing IOUs 5-18
Viewing IOCs 5-19
Viewing All IOCs 5-19
Viewing IOC Properties 5-19
Viewing IOC Services 5-21
Viewing All IOC Services 5-21
Viewing Properties of IOC Services 5-21

CHAPTER 6 Ethernet Tasks 6-1

Viewing and Managing Bridge Groups 6-1

Viewing Bridge Groups 6-1
Viewing Bridge Group Properties 6-2
Adding Bridge Groups 6-3
Configuring Bridge Groups 6-4
Deleting Bridge Groups 6-5
Viewing and Managing Bridge Subnets 6-5
Viewing Bridge Subnets 6-5
Adding a Bridge Subnet 6-6
Deleting a Bridge Subnet 6-6
Viewing and Managing Bridge Forwarding 6-6
Viewing Bridge Forwarding 6-6
Adding Bridge Forwarding 6-7
Deleting Bridge Forwarding 6-7
Viewing and Managing Redundancy Groups 6-8
Viewing Redundancy Groups 6-8
Creating a Redundancy Group 6-9
Deleting a Redundancy Group 6-10
Viewing or Editing Redundancy Group Properties 6-10
Viewing and Managing Trunk Groups 6-11
Viewing Trunk Groups 6-11
Adding a Trunk Group 6-13
Configuring a Trunk Group 6-13
Deleting a Trunk Group 6-14

CHAPTER 7 **Fibre Channel Tasks** 7-1

Configuring Global ITL Attributes 7-1
Viewing and Managing SRP Hosts (Initiators) 7-2
Viewing SRP Hosts (Initiators) 7-3
Viewing SRP Host (Initiator) Properties 7-3
Viewing SRP Host (Initiator) World-Wide Port Names 7-4
Viewing IT Policies of the Host 7-4
Viewing ITL Policies of the Host 7-5
Adding a SRP Host 7-5
Deleting a SRP Host 7-6
Configuring SRP Host (Initiator) Properties 7-6
Viewing and Configuring Fibre Channel Targets 7-7
Viewing Fibre Channel Targets 7-7
Viewing Fibre Channel Target Properties 7-7
Configuring Fibre Channel Target Properties 7-8

Viewing IT Policies of the Target 7-9
Viewing ITL Policies of the Target 7-9
Viewing and Managing Fibre Channel LUNs 7-9
Viewing Fibre Channel LUNs 7-10
Viewing Fibre Channel LUN Properties 7-10
Configuring Fibre Channel LUN Properties 7-11
Viewing ITL Policies of the LUN 7-12
Viewing ITs and IT Properties 7-12
Viewing ITs 7-12
Viewing IT Properties 7-13
Viewing ITLs and ITL Properties 7-14
Viewing ITLs 7-14
Viewing ITL Properties 7-14
Viewing Global Statistics 7-15

INDEX

Preface

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

- Audience, page ix
- Organization, page ix
- Conventions, page x
- Related Documentation, page xi
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xi

Audience

The intended audience is the administrator responsible for installing, configuring, and managing server 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 Chassis Manager	Describes Chassis Manager fundamentals.
Chapter 2	Getting Started	Describes how to get started with Chassis Manager.
Chapter 3	Chassis Tasks	Describes how to view the component status on the chassis and configure ports.
Chapter 4	Maintenance Tasks	Describes the tasks for configuring the basic system operation.
Chapter 5	InfiniBand Tasks	Describes the tasks for displaying and configuring the InfiniBand operation.

Chapter	Title	Description
Chapter 6	Ethernet Tasks	Describes the tasks for displaying and configuring the Ethernet operation.
Chapter 7	Fibre Channel Tasks	Describes the tasks for displaying and configuring the Fibre Channel operation.

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.
`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:
  - *Release Notes for Cisco SFS 7000D Series Switch Software Release 2.9.0*
  - *Cisco SFS Product Family Element Manager User Guide*
  - *Cisco SFS Product Family Command Reference*
- For detailed hardware configuration and maintenance procedures, see these hardware guides:
  - *Cisco SFS 7000D InfiniBand Server Switch Installation and Configuration Note*
  - *Cisco SFS 7000D InfiniBand Server 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 Chassis Manager

Chassis Manager runs directly on Cisco SFS Server Switches to perform administration tasks. These topics introduce the various components of the interface:

- Introduction, page 1-1
- Browser Requirements, page 1-7
- Platform Requirements, page 1-8

Introduction

Chassis Manager runs in a standard web browser and displays information in standard HTML formats. The GUI has three frames:

- System Frame, page 1-1 (See Figure 1-1.)
- Tree Frame, page 1-2 (See Figure 1-2.)
- View Frame, page 1-6 (See Figure 1-4.)

System Frame

The System frame displays and updates the status of the cards, power supplies, and fans in your device. Each number in the Cards, Power Supplies, and Fans fields identifies a field-replaceable unit (FRU) in your device based on the slot number in which it resides. The color of the slot number indicates the status of the FRU. Figure 1-1 shows a system frame for an SFS 7008P Server Switch.

Figure 1-1 System Frame

Table 1-1 lists the colors in the display and explains what each color indicates.

Table 1-1 FRU Color Indicators

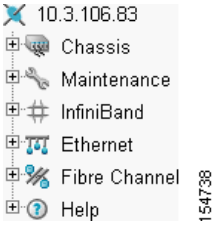
Color	Indication
green	Operational and administrative status of up.
gray	Administrative status of down.
red	Operational status of down.

- Launch a CLI session to the server switch by clicking the IP address in the IP Address field to open a Telnet window.
- Contact Cisco TAC from the Support Contact field by clicking the e-mail address and sending an e-mail message.
- Start the online help by clicking on **Help**.

Tree Frame

The Tree frame appears on the lower left of the Chassis Manager display and provides a navigation tree that groups the functional branches of your device under icons. Figure 1-2 displays the Tree frame on a Cisco SFS 3001 Server Switch.

Figure 1-2 Tree Frame



Note Figure 1-2 displays a tree frame for a user with unrestricted access. Restricted users may see fewer icons. For more information, see the "Understanding Access Privileges" section on page 2-9.

Table 1-2 describes the icons in the Tree frame.

Table 1-2 Tree Frame Icons

Icon	Description
Chassis ( )	The Chassis icon lets you view and configure hardware in your server switch. Access this icon to view the status of all field-replaceable units (FRUs) on your device.
Maintenance ( )	The Maintenance icon contains branches that let you perform basic administrative tasks on your server switch. Access this icon to configure Network Time Protocol (NTP) servers, assign a boot-config file, view the contents of the file system, and so on.

Table 1-2 Tree Frame Icons (continued)

Icon	Description
InfiniBand ( )	The InfiniBand icon provides subnet manager and I/O details. You can click the Subnet Manager branch of this icon to configure basic subnet manager properties.
Ethernet ( ) (select hardware platforms only)	The Ethernet icon lets you view and configure many aspects of IP traffic on your server switch.
Fibre Channel ( ) (select hardware platforms only)	The Fibre Channel icon shows your SRP host and Fibre Channel storage details and lets you configure global policies.
Help ( )	The Help icon takes you to online help and support resources.

Click a plus-sign icon ( ) to expand an icon and display the branches that you can configure. After you expand an icon, click a branch icon ( ) to open the configuration options for that branch in the View frame.

Table 1-3 describes the configurable branches under the Chassis icon.

Table 1-3 Chassis Icon Branches

Branch	Description
Cards	Click this branch to display and configure controller, switch, and gateway cards.
Ports	Click this branch to display and configure all external InfiniBand, Ethernet, and Fibre Channel ports on your device.
Power Supplies (select hardware platforms only)	Click this branch to view the status of the power supplies on your device.
Fans (select hardware platforms only)	Click this branch to view the status of the fans on your device.
Sensors	Click this branch to view the status and readings on the temperature sensors on your device.
Backplane (select hardware platforms only)	Click this branch to view backplane details.
Management Ports	Expand the Management Ports icon to display the following branches: • Serial displays the Serial Console port configuration. • Ethernet displays the Ethernet Management port configuration. • InfiniBand displays the InfiniBand Management port configuration.

Table 1-4 describes the configurable branches under the Maintenance icon.

Table 1-4 Maintenance Icon Branches

Branch	Description
System Information	Click this branch to view and configure the information that appears in the System frame.
System Global Settings	Click this branch to view the system global settings.
Time	Click this branch to configure the time and date on your server switch and to assign NTP servers to your device.
File Management	Click this branch to view, import, export, and install files in the file system on your device.
Boot Configuration	Click this branch to select a configuration for your server switch to use when it boots.
Backup Configuration	Click this branch to save your running configuration to a file.
Save Config	Click this branch to save the running configuration as the startup configuration. When your server switch reboots, it runs the updated configuration.
Reboot	Click this branch when you want to reload your server switch.
Services	Expand the Services icon to display the following branches: • General Displays the following system services and lets you configure them: – DNS – FTP – Telnet – Syslog – RADIUS – TACACS+ • HTTP Displays HTTP properties and configuration options. • Radius Servers Displays the RADIUS server(s) that your device can use to authenticate user logins and lets you configure attributes of the server(s). • Tacacs Servers Displays the TACACS+ server(s) that your device can use to authenticate user logins and lets you configure attributes of the server(s). • Authentication Failures Lists CLI, SNMP, and HTTP authentication failures.
Diagnostics	Expand this branch to view server switch diagnostic data in the following branches: • POST • Fru Error

Table 1-5 describes the configurable branches under the InfiniBand icon.

Table 1-5 InfiniBand Icon Branches

Branch	Description
Subnet Managers	Click this branch to view and configure the subnet managers in your fabric.
Services	Click this branch to view the IB fabric services that have registered with the subnet manager.
Topology	Expand the Topology icon to display the following branches: • Nodes Click this branch to view the IB nodes in your IB fabric. • Ports Click this branch to view the IB ports in your IB fabric. • Neighbors Click this branch to display the interconnecting IB nodes and relevant ports in your IB fabric.
Device Management (select hardware platforms only)	Expand the Device Management icon to display the following branches: • IOU Click this branch to view the I/O unit on your server switch. • IOCs Click this branch to view the controller(s) on your device. • IOC Services Click this branch to view the IB features on your device.

Table 1-6 describes the configurable branches under the Ethernet icon.

Table 1-6 Ethernet Icon Branches

Branch	Description
Bridge Groups	Click this branch to view bridge groups on your server switch.
Bridge Subnet	Click this branch to view the subnets of bridge groups.
Bridge Forwarding	Click this branch to view the forwarding properties of bridge groups.
Redundancy Group	Click this branch to view redundancy groups.
Trunk Groups	Click this branch to view trunk groups on your server switch.

Table 1-7 describes the configurable branches under the Fibre Channel icon.

Table 1-7 Fibre Channel Icon Branches

Branch	Description
Global Policies	Click this branch to view and configure the default attributes of new IB-to-FC connections.
SRP Hosts	Click this branch to view and configure SRP hosts that serve as initiators for SAN fabrics.
Targets	Click this branch to view and configure Fibre Channel targets that connect to your server switch through FC gateways.
Logical Units	Click this branch to view and configure Fibre Channel LUNs that connect to your server switch through FC gateways.
ITs	Click this branch to view and configure attributes of initiator-target connections.
ITLs	Click this branch to view and configure attributes of initiator-target-LUN connections.
Global Statistics	Click this branch to view IB-to-FC traffic statistics.

Table 1-8 describes the configurable branches under the Help icon.

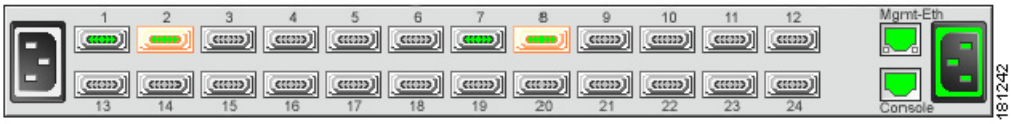
Table 1-8 Help Icon Branches

Branch	Description
Help Index	Click this branch to launch Chassis Manager online help.
Support	Click this branch to open the support website.

View Frame

The View frame appears on the right of the interface. Input fields and device details appear in this frame. The contents of the View frame vary based on the branch that you click in the Tree frame. Figure 1-3 displays the graphic of the cable end, or service end, of the chassis that appears in the View frame when you first log in to the chassis manager.

Figure 1-3 View Frame on Logon

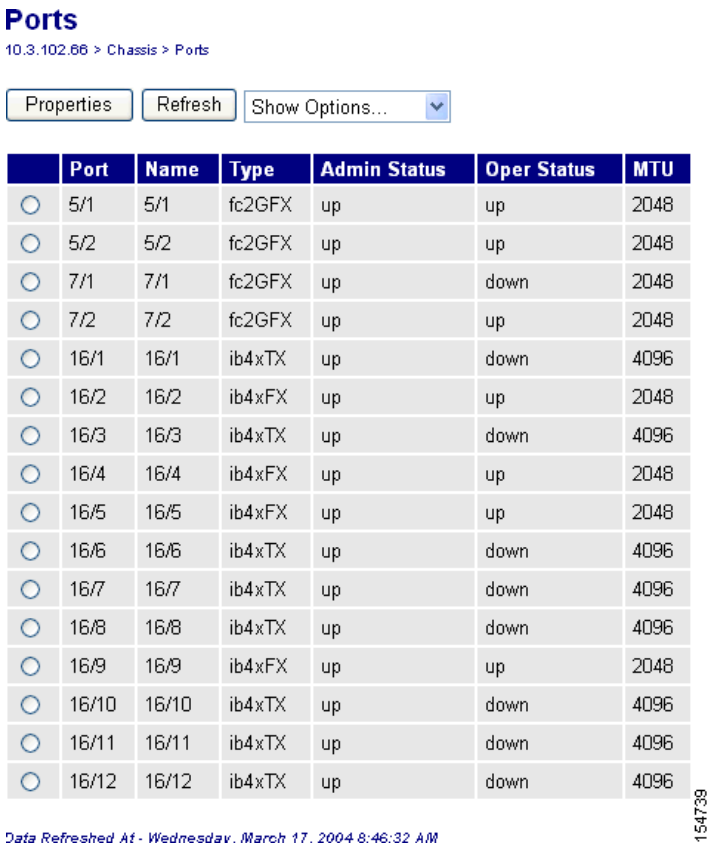


Ports 1 through 24 are InfiniBand ports.

- 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.

Figure 1-4 shows another View Frame example. You get this display when you expand **Chassis** in the tree frame and then click the **Ports** branch.

Figure 1-4 View Frame Example



Browser Requirements

Chassis Manager supports the following browsers:

- Microsoft Internet Explorer Version 6
- Netscape Navigator Version 6
- Mozilla Version 1.4

Platform Requirements

Chassis Manager runs on the following platforms:

- Windows
- Solaris
- Linux

CHAPTER 2

Getting Started

This chapter describes how to get started using Chassis Manager and contains these sections:

- Preparing Your Device, page 2-1
- Launching Chassis Manager, page 2-4
- Navigating Chassis Manager, page 2-8
- Understanding Access Privileges, page 2-9
- Viewing the Device Status, page 2-9

Preparing Your Device

To launch Chassis Manager on your server switch, you must complete the following tasks:

- Configure an IP address on the Ethernet management port.
- Configure an IP gateway on the Ethernet management port.
- Enable HTTP and/or HTTPS services.

Note Chassis Manager optionally supports Secure Sockets Layer (SSL) secure connections.

If your device meets these requirements, proceed to the "Launching Chassis Manager" section on page 2-4. Otherwise, the steps required to prepare your device are platform dependent.

Configuring an IP address can be done statically or dynamically using a Dynamic Host Configuration Protocol (DHCP) server. On Cisco SFS 7000D Server Switches, DHCP is enabled by default. Static configuration is the default on all other server switches.

These topics describe how to prepare your device:

- Configuring an IP Address for a Cisco SFS 7000D Server Switch Using DHCP, page 2-2
- Configuring a Static IP Address, page 2-2
- Configuring an IP Address Dynamically on a Device for which DHCP is not the Default, page 2-3
- Enabling HTTP or HTTPS Services, page 2-4

Note Consult your network administrator for an IP address, subnet mask, and gateway address before you begin this process.

Configuring an IP Address for a Cisco SFS 7000D Server Switch Using DHCP

By default, the Cisco SFS 7000D Server Switch obtains an IP address and gateway automatically and dynamically from a DHCP server. The DHCP server must be configured to the MAC address of your server switch, which is printed on top of the server switch chassis.

You can override the default and configure a static IP address for your Cisco SFS 7000D Server switch as described in "Configuring a Static IP Address".

Configuring a Static IP Address

To configure a static IP address for your server switch, follow these steps:

Step 1 Use the Serial Console port to open a CLI session to your device, and then log in as a user with administrative access.

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

```
SFS-7000> enable
SFS-7000#
```

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

```
SFS-7000# configure terminal
SFS-7000(config)#
```

Step 4 Enter the **interface mgmt-ethernet** command to enter Ethernet management interface configuration submode.

```
SFS-7000(config)# interface mgmt-ethernet
SFS-7000(config-if-mgmt-ethernet)#
```

Step 5 On Cisco SFS 7000D Server Switches, enable the static address option, which turns off the default-enabled DHCP. Omit this step for all other server switches.

```
SFS-7000D(config)# address-option static
```

Step 6 Enter the **ip address** command and an address and subnet mask. Consult your network administrator for an IP address. You will use this address in your web browser to launch Chassis Manager.

```
SFS-7000(config-if-mgmt-ethernet)# ip address 10.3.102.66 255.255.0.0
```

Step 7 Enter the **gateway** command and then a default IP gateway. Consult your network administrator for a gateway address.

```
SFS-7000(config-if-mgmt-ethernet)# gateway 10.3.0.1
```

Step 8 Enter the **no shutdown** command to enable the Ethernet Management port.

```
SFS-7000(config-if-mgmt-ethernet)# no shutdown
```

Step 9 Enter the **exit** command to return to global configuration mode.

```
SFS-7000(config-if-mgmt-ethernet)# exit
```

Configuring an IP Address Dynamically on a Device for which DHCP is not the Default

To use a DHCP server to configure a dynamic IP address for a device other than a Cisco SFS 7000D Server Switch, follow these steps:

Step 1 Enter the **enable** command.

```
SFS-3012R> enable
SFS-3012R#
```

Step 2 Enter the **configure** command.

```
SFS-3012R# configure
SFS-3012R(config)#
```

Step 3 Enter the **interface mgmt-ethernet** command.

```
SFS-3012R(config)# interface mgmt-ethernet
```

Step 4 Enter the **addr-option dhcp** command to configure the chassis to obtain the IP address from the DHCP server.

```
SFS-3012R(config-if-mgmt-ethernet)# addr-option dhcp
```

Step 5 Enable the management port with the **no shutdown** command.

```
SFS-3012R(config-if-mgmt-ethernet)# no shutdown
```

Step 6 Save the configuration to preserve it between reboots.

```
SFS-3012R(config-if-mgmt-ethernet)# exit
SFS-3012R(config)# exit
SFS-3012R# copy running-config startup-config
```

Step 7 Enter the **show interface mgmt-ethernet** command to determine your IP address, as shown in the following example:

```
SFS-3012R# show interface mgmt-ethernet


================================================================================
                          Mgmt-Ethernet Information
================================================================================
             mac-address : 00:05:ad:00:1e:1c
          auto-negotiate : enabled
            admin-status : up
             oper-status : up
                 ip-addr : 172.29.230.60
                    mask : 255.255.0.0
            gateway-addr : 172.29.230.1
             addr-option : static
```

Enabling HTTP or HTTPS Services

To enable HTTP or STTPS services, follow these steps:

Step 1 (Optional) Enter the **ip http server** command to enable HTTP services on your device to permit unsecured access to your server switch.

```
SFS-7000(config)# ip http server
```

Step 2 (Optional) Enter the **ip http secure-server** command to enable HTTPS services on your device to permit SSL-secured access to your server switch.

```
SFS-7000(config)# ip http secure-server
```

Launching Chassis Manager

Chassis Manager without SSL requires no additional setup. Chassis Manager with SSL requires additional steps based on your browser. These topics describe how to complete these procedures:

- Launching Chassis Manager without SSL, page 2-4
- Launching Chassis Manager with SSL, page 2-5
- Avoiding Error Messages, page 2-7
- Logging Out of Chassis Manager, page 2-8

Launching Chassis Manager without SSL

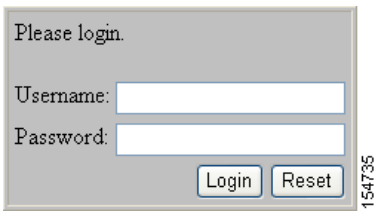
To launch Chassis Manager without SSL, follow these steps:

Step 1 Launch your web browser.

Step 2 Type the IP address of your server switch in the address field of your browser, and press **Enter**. (You configured the IP address in the Step 6 of "Preparing Your Device" section on page 2-1.)

A login window opens. Figure 2-1 displays the login window.

Figure 2-1 Chassis Manager Login Window



Step 3 Enter your server switch username and password in the login window, and click **Login**.

Chassis Manager loads in your browser window.

Launching Chassis Manager with SSL

SSL setups vary by browser types. These topics explain how to launch Chassis Manager with SSL using particular browsers:

- Netscape/Mozilla, page 2-5
- Internet Explorer, page 2-5

Netscape/Mozilla

To launch a secure Chassis Manager connection using the Netscape/Mozilla browser, follow these steps:

Step 1 Launch your web browser.

Step 2 Type **https://** and the IP address of your server switch in the address field of your browser, and press **Enter**. (You configured the IP address in Step 6 of the "Preparing Your Device" section on page 2-1.)

A login window opens.

Step 3 Click **Yes** or **OK** to close any browser messages.

Mozilla dynamically manages your certificate.

Step 4 Enter your server switch username and password in the login window, and click **Login**.

Chassis Manager loads in your browser window.

Internet Explorer

To launch a secure Chassis Manager connection using the Internet Explorer browser, follow these steps:

Step 1 Launch your web browser.

Step 2 Type **https://** and the IP address of your server switch in the address field of your browser.

(You configured the IP address in Step 6 of "Preparing Your Device" section on page 2-1.)

Step 3 Press **Enter**.

A Security Alert window opens.

Figure 2-2 Security Alert Window

Step 4 Click **View Certificate**.

The Certificate window opens.

Step 5 Click the **Certification Path** tab.

Step 6 Click the root certificate in the tree.

You see the tab in Figure 2-3.

Step 7 Click **View Certificate**.

Step 8 Click **Install Certificate**.

Step 9 Click **Next**.

Step 10 Choose **Place all certificates in the following store**.

Step 11 Click **Browse**.

The Select Certificate Store window opens.

Step 12 Click **Trusted Root Certification Authorities**, and then click **OK**.

Step 13 Click **Next**, and then click **Finish**.

Figure 2-3 Certification Path

Avoiding Error Messages

By default, SSL certificates map to the IP address of the Ethernet Management port of a server switch. If you enter the system name of your host (that you configure with the **hostname** command) or the IP address of the InfiniBand Management Port of your server switch to launch Chassis Manager, your browser displays an alert. The alert cautions you that the name on the certificate does not match the name of the site. This hostname mismatch message reappears after you log in and the java applet begins to load. To avoid this message entirely, configure your server switch to use the identifier that you enter in the browser to verify certificates.

To configure the certificate name to use the system name, follow these steps:

Step 1 Establish a Telnet session to your server switch, and log in as a user with administrative privileges.

```
Login: super
Password: xxxxx
```

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

```
SFS-7000D> enable
SFS-7000D#
```

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

```
SFS-7000D# configure terminal
SFS-7000D(config)#
```

Step 4 Enter the **ip http** command with the **secure-cert-common-name** keyword and the system name (hostname) of the server switch to configure your certificates to use the system name of your server switch.

```
SFS-7000D(config)# ip http secure-cert-common-name useSysName
```

When you open Chassis Manager with the system name of your server switch, error messages will not repeatedly appear.

Logging Out of Chassis Manager

To log out of Chassis Manager, close the web browser window that displays the GUI. If you have multiple windows open (such as the main window and a properties window), close all of the windows.

Navigating Chassis Manager

The Tree frame of the web-based interface provides a high-level map of Chassis Manager. As you move from display to display in Chassis Manager, the View frame constantly reminds you where you are in the system.

When you click a branch in the Tree frame, the title of the display that appears in the View frame matches the name of the branch. Directly below the display title appears a tiered locator that details the level of the current display in relation to other elements of Chassis Manager. For instance, when you click the Cards branch of the Chassis icon, the following locator string appears:

A.B.C.D > Chassis > Cards

In this instance, *A.B.C.D* represents the IP address of your server switch. The tiered locator indicates that your current display is the Cards display, which is a branch of the Chassis icon on the device with an IP address of *A.B.C.D*.

When you further filter your display, the View frame indicates the new level of granularity. For instance, if you view the ports on a particular gateway card instead of all ports on the device, a tiered locator appears, followed by a filter indicator. If you view only external ports on an Ethernet gateway in slot 4, the following identifiers appear:

A.B.C.D > Chassis > Ports

Filter : Card = 4

The second identifier indicates that the display shows only the ports on Card 4.

These topics provide more information about navigating Chassis Manager:

- Moving Backward, page 2-9
- Refreshing Views, page 2-9

Moving Backward

Because no formal “move backward” function exists in Chassis Manager, use one of the following options to return to a previous display:

- Click **Back** on your web browser.
- Right-click in the View frame, and choose **Back** from the drop-down menu.
- Navigate to the desired display with the Tree frame.

Note When you use the Back function of your web browser, your browser may not cache selections that you made for a particular view. For instance, if you view the gateway ports of a card and then click a branch in the Tree frame, your previous display may not appear correctly when you click the Back button.

Refreshing Views

Chassis Manager lets you update most displays to reflect changes that occurred since you opened the display. To refresh your view, click the **Refresh** button in your display.

Understanding Access Privileges

The functionality available to you from Chassis Manager varies based on the access privileges of your username. If you do not have read access to a particular technology, the icon and branches for that technology do not appear in your GUI. If you do not have write access to a particular technology, the configuration options for that technology do not appear in your GUI.

Viewing the Device Status

Chassis Manager provides an overview of the status of the components of your server switch.

Note To view the status summary of your device, click the IP address at the top of the Tree frame.

Items that appear in green are active. Items that appear in gray are not active. Items that appear in red are faulty or administratively down.

CHAPTER 3

Chassis Tasks

These topics describe the Chassis display tasks:

- Viewing Cards on a Chassis, page 3-1
- Viewing Internal Gateway Ports, page 3-7
- Viewing Physical Ports on a Chassis, page 3-8
- Configuring Ports, page 3-13
- Viewing Power Supply Status, page 3-15
- Viewing Fan Status, page 3-17
- Viewing Temperature Sensor Status, page 3-18
- Viewing the Backplane Information, page 3-19
- Viewing Management Ports on a Chassis, page 3-19
- Setting the Partition for the InfiniBand Management Port, page 3-21

Viewing Cards on a Chassis

These topics describe how to view information about cards in the chassis and set the up/down administrative status of a card:

- Viewing Card Summary Information, page 3-1
- Viewing Card Properties, page 3-3
- Viewing the Card Inventory, page 3-6
- Configuring the Administrative Status of a Card, page 3-7

Viewing Card Summary Information

To view the cards on your chassis, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Cards** branch.

A table that includes all cards on the chassis appears in the View frame. Table 3-1 describes the fields in the Cards table.

Table 3-1 Cards Table Field Descriptions

Field	Description
Slot	Number of the chassis slot in which the card resides.
Type	Type of the card.
Current 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 • bootFailed • tooHot • booting • checkingBootImage • wrongBootImage • rebooting • standby • recoveryImage 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 wrongBootImage 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. The tooHot condition indicates that the card is overheating. Expand **Chassis** and select the **Fans** branch to see if your fans have failed. The booting condition indicates that the card has not finished loading the necessary image data for the internal configuration.

Table 3-1 Cards Table Field Descriptions (continued)

Field	Description
Boot Stage	Boot Stage appears as one of the following: • recovery • ipl • ppcboot • fpga • pic • ib • rootfs • kernel • exe • done • none
Boot Status	Boot Status may appear as any of the following: • upgrading • success • failed • badVersion • badCrc • memoryError • outOfSpace • programmingError • hardwareError • fileNotFound • inProgress • none

Step 3 (Optional) Click **Refresh** to update the attributes in the display.

Viewing Card Properties

To view card properties, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Cards** branch.

A Cards table that includes all cards in the chassis appears. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the card with properties you want to view.

Step 4 Click **Properties**.

A Card Properties window opens. Table 3-2 describes the fields in the Card Properties window.

Table 3-2 Card Properties Window Field Descriptions

Field	Description
Slot ID	Number of the chassis slot in which the card resides.
Type	Type of the card.
Admin Status	Displays the up and down radio buttons. Click a radio button, and then click **Apply** to change the administrative status and bring up or bring down the port.
Current 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 be any of the following: • unknown • normal • wrong-image • 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. If your card overheats, the tooHot condition appears in the **show card** command output. Enter the **show fan** command to check if your fans have failed. The booting condition indicates that the card has not finished loading necessary image data for internal configuration.
Boot Stage	Boot Stage appears as one of the following: • recovery • ipl • ppcboot • fpga • pic • ib • rootfs • kernel • exe • done • none

Table 3-2 Card Properties Window Field Descriptions (continued)

Field	Description
Boot Status field	Boot Status may appear as 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) number of the card.
FRU Number	Field-replaceable unit (FRU) number of the card.
Product Version ID	The ID number of the version of the card.
Action (select cards only)	Radio buttons list actions that you can apply to the card.
Result (select cards only)	Result that occurs when you choose an action from the Action field and click **Apply**.

Viewing the Card Inventory

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

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Cards** branch.

The Cards table appears.

Step 3 Click the radio button next to the card with inventory you want to view.

Step 4 Click **Inventory**.

The Card Inventory window opens. Table 3-3 describes the fields in this window.

Table 3-3 Card Inventory Window Field Descriptions

Field	Description
Slot ID	Slot on the server switch in which the card resides.
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.
PIC Firmware Revision (select cards)	Current PIC firmware version that the card runs.
FPGA Firmware Revision (select cards)	Current FPGA firmware version that the card runs.
IB Firmware Revision	Version of InfiniBand firmware on the card. For platforms designed with the InfiniScale III switch chip (7000 and 7008 platforms), the Chassis 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.
Card Uptime	How long, in seconds, the card has been running.
Close	Closes the Card Inventory window.
Help	Opens the online help.

Configuring the Administrative Status of a Card

With Chassis Manager, you can bring up or shut down any card on your chassis. To configure the administrative status of a card, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Cards** branch.

A table of the cards in the chassis appears. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the card that you want to configure.

Step 4 Click **Properties**.

A Card Properties window opens.

Step 5 In the Admin Status field, click the **up** or **down** radio button, and then click **Apply**.

Viewing Internal Gateway Ports

Each Fibre Channel gateway and Ethernet gateway uses two internal ports to pass traffic through your device.

Note Not all hardware platforms provide this option.

To view gateway port details, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Cards** branch.

A Cards table that includes all cards in the chassis appears. A radio button appears to the left of each table entry.

Step 3 Click the radio button to the left of the card with gateway (internal) ports you want to view.

Step 4 From the Show Options drop-down menu, choose **Show Gateway Ports**.

The Gateway Ports table opens in the View frame. For a description of the fields in the Gateway Ports table, see Table 3-4.

Table 3-4 Gateway Ports Table Field Descriptions

Field	Description
GW Port	Port number, in slot#/port# format.
Name	Port name.
Type	Port type.

Viewing Physical Ports on a Chassis

These topics describe how to view ports on a chassis:

- Viewing All Ports, page 3-8
- Viewing Port Properties, page 3-8
- Viewing Port Bridging Properties, page 3-11
- Viewing Port Statistics, page 3-11

Viewing All Ports

To view the physical ports on your device, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

A table that includes all ports on the chassis appears in the View frame. Table 3-5 describes the fields in the Ports table.

Table 3-5 Ports Display Field Descriptions

Field	Description
Port	Slot#/port# identifier of the port.
Name	User-configured port name.
Type	Displays the type of the port. Type names begin with fc to indicate Fibre Channel, en to indicate Ethernet, and ib to indicate InfiniBand.
Admin Status	Displays up when you bring up the port; otherwise, displays down.
Oper Status	Indicates whether or not the port is ready for use.
MTU	Maximum transmission unit (MTU) of the port, in bytes.

Step 3 (Optional) Click **Refresh** to update the attributes in the display.

Viewing Port Properties

To view port properties, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

A Ports table that includes all ports in the chassis appears. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the port with properties you want to view.

Step 4 Click **Properties**.

The Port Properties window opens. Each type of port displays different properties in this window.

Note Available port types vary by hardware platform.

Table 3-6 describes the fields in the Port Properties window of an Ethernet port.

Table 3-6 Ethernet Port Properties Window Field Descriptions

Field	Description
Port	Port number in slot#/port# notation.
Name	Port name that you can edit and apply to the port.
Type	Type of the port.
Admin Status	Configures the administrative status of the port with up and down radio buttons.
Oper Status	Indicates whether or not the port is ready for use.
Auto Negotiation Supported	Displays true if the port supports auto-negotiation.
Auto Negotiation	The Enable check box enables or disables auto-negotiation on the port.
Set Port Speed	Radio buttons that let you configure the speed of the port.
Current Speed	Displays the speed of the port.
Set Port Duplex	(Ethernet Gateway ports) Radio buttons configure duplex setting of the port.
Current Duplex	(Ethernet Gateway ports) Indicates whether the port runs in full duplex mode or half duplex mode.
MTU field	Displays the maximum transmission unit (MTU) of the port in bytes.
MAC Address	(Ethernet Gateway ports) Flushes the address resolution protocol table.
Last Changed On	Time and date of the last time that the port was configured.
Action	(Ethernet Gateway ports) Flushes the address resolution protocol table.
Result	(Ethernet Gateway ports) Displays result of the action in the Action field.

Table 3-7 describes the fields in the Port Properties window of a Fibre Channel port.

Table 3-7 Fibre Channel Port Properties Window Field Descriptions

Field	Description
Port	Port number in slot#/port# notation.
Name	Port name that you can edit and apply to the port.
Type	Displays the type of the port.

Table 3-7 Fibre Channel Port Properties Window Field Descriptions (continued)

Field	Description
Admin Status	Up and down radio buttons that configure the administrative status of the port.
Oper Status	Displays up to indicate that the port is physically ready for use, otherwise displays down.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Auto Negotiation	The Enable check box enables or disables autonegotiation on the port.
Set Port Speed	1G and 2G radio buttons configure the port speed.
Current Speed	Displays the speed of the port.
Current Connection Type	Type of connection that the server switch dynamically discovered for this port.
MTU	Maximum transmission unit (MTU) of the port, in bytes.
WWNN	World-wide node name (WWNN) of your device.
WWPN	World-wide port name (WWPN) of the port.
FC ID	Fibre Channel Protocol (FCP) identifier of the port.
Last Changed On	Time and date of the last time that a user configured the port.

Table 3-8 describes the fields in the Port Properties window of an InfiniBand port.

Table 3-8 InfiniBand Port Properties Window Field Descriptions

Field	Description
Port	Port number in slot#/port# notation.
Name	Port name that you can edit and apply to the port.
Type	Type of the port.
Admin Status	Up and down radio buttons configure the administrative status of the port.
Oper Status	Displays up to indicate that the port is physically ready for use; otherwise, displays down.
Auto Negotiation Supported	Displays true if the port supports autonegotiation.
Auto Negotiation	Enable check box enables or disables 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 options are 1x-SDR (2.5 Gbps), 4x-SDR (10 Gbps), 12x-SDR (30 Gbps), 1x-DDR (5 Gbps), 4x-DDR (20 Gbps), 12x-DDR (60 Gbps). **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 SDR only.
Current Speed	Link capacity of the port.
Physical State	Physical state of the port.

Table 3-8 InfiniBand Port Properties Window Field Descriptions (continued)

Field	Description
Clear Counters	Check box allows you to clear the counters for the InfiniBand port.
MTU	Maximum transmission unit (MTU) of the port in bytes.
Last Changed On	Time and date of the last time that a user configured the port.

Viewing Port Bridging Properties

To view the bridge to which a port belongs, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

A Ports table appears that includes all ports in the chassis. A radio button appears to the left of each table entry.

Step 3 Click the radio button next to the port with bridging properties you want to view.

Step 4 Choose **Show Bridging** from the Show Options drop-down menu.

The Port Bridging table appears in the View frame. Table 3-9 describes the fields in this table.

Table 3-9 Port Bridging Table Field Descriptions

Field	Description
Port	Port that you chose from the Ports table.
Vlan	Virtual LAN (VLAN) of the bridge to which the port belongs.
Bridge ID	Bridge ID of the bridge to which the port belongs.

Viewing Port Statistics

To view port statistics, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

The Ports table appears in the View frame.

Step 3 Click the radio button next to the port with statistics you want to view.

Step 4 Choose **Show Port Statistics** from the Show Options drop-down menu.

The Port Statistics display appears in the View frame. Table 3-10 describes the fields in this display.

Table 3-10 Port Statistics Display Field Descriptions

Field	Description
Port	Port number, as assigned by the subnet manager.
Name	Administratively assigned port name.
In Octets	Cumulative number of octets that arrived at the port, including framing characters.
In Unicast Packets	Cumulative number of incoming packets destined for a single port.
In Multicast Packets	Cumulative number of incoming packets destined for the ports of a multicast group.
In Broadcast Packets	Cumulative number of incoming packets destined for all ports on the fabric.
In Discards	Cumulative number of inbound packets that the port discarded for a reason other than a packet error (lack of buffer space).
In Errors	Number of inbound packets with errors that the port discarded.
In Unknown Protocols	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.
Out Octets	Total number of octets transmitted out of the interface, including framing characters.
Out Unicast Packets	Total number of packets that higher-level protocols requested be transmitted and were not addressed to a multicast or broadcast address at this sublayer, including those packets that were discarded or not sent.
Out Multicast Packets	Total number of packets that higher-level protocols requested be transmitted and were addressed to a multicast address at this sublayer, including those packets that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses.
Out Broadcast Packets	Total number of packets that higher-level protocols requested to be transmitted and were addressed to a broadcast address at this sub-layer, including those packets that were discarded or not sent.
Out Discards	Number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their transmission. One possible reason for discarding such a packet could be to free buffer space.
Out Errors	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 Ports

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

These topics describe how to configure port properties:

- Configuring a Port Name, page 3-13
- Enabling or Disabling a Port, page 3-13
- Configuring Autonegotiation on a Port, page 3-14
- Configuring Port Speed, page 3-14
- Clearing InfiniBand Port Counters, page 3-15

Configuring a Port Name

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

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

The Ports table appears in the View frame. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the port to which you want to assign a name.

Step 4 Click **Properties**.

The Port Properties window opens.

Step 5 In the Name field of the Port Properties window, enter a name for the port, and then click **Apply**.

Step 6 Click **Close** to close the Port Properties window.

Enabling or Disabling a Port

To enable or disable a port, follow these steps:

Step 1 Expand the **Chassis** icon in the Tree frame.

Step 2 Select the **Ports** branch.

The Ports table appears in the View frame. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the port you want to enable or disable.

Step 4 Click **Properties**.

The Port Properties window opens.

Step 5 In the Admin Status field of the Port Properties window, click the **up** (enable) or **down** (disable) radio button, and then click **Apply**.

Step 6 Click **Close** to close the Port Properties window.

Configuring Autonegotiation on a Port

To enable or disable auto-negotiation on a port, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

The Ports table appears in the View frame. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the port for which you want to enable or disable autonegotiation.

Step 4 Click **Properties**.

The Port Properties window opens.

Step 5 In the Auto Negotiation field of the Port Properties window, check the **Enable** check box to enable it, or uncheck the check box to disable it, and then click **Apply**.

Step 6 Click **Close** to close the Port Properties window.

Configuring Port Speed

Note You must disable autonegotiation before configuring the port speed.

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.

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

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Ports** branch.

The Ports table appears in the View frame. A radio button appears to the left of each table entry.

Step 3 Click the radio button of the port for which you want to configure the speed.

Step 4 Click **Properties**.

The Port Properties window opens.

Step 5 In the Auto Negotiation field, uncheck the **Enable** check box (if necessary) to disable autonegotiation.

Step 6 In the Set Port Speed field of the Port Properties 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 7 Click **Apply**.

Step 8 Click **Close** to close the Port Properties window.

Clearing InfiniBand Port Counters

To clear InfiniBand port counters, follow these steps:

Step 1 Expand **Chassis** in the Tree frame, and select the **Ports** branch.

The Ports table appears in the View frame. A radio button appears to the left of each table entry.

Step 2 Click the radio button of the port for which you want to clear the counters.

Step 3 Click **Properties**.

The Port Properties window opens.

Step 4 Check the **Clear Counters** check box.

Step 5 Click **Apply**, and then click **Close**.

See Table 3-10 on page 3-12 for descriptions of the counters cleared by this procedure.

Viewing Power Supply Status

These topics describe how to view information about power supplies:

- Viewing Power Supply Summary Information, page 3-15
- Viewing Power Supply Properties, page 3-16

Viewing Power Supply Summary Information

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

Note Not all hardware platforms include power supply information. In such cases, the Power Supplies branch does not appear.

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Power Supplies** branch.

The Power Supplies table appears in the View frame. Table 3-11 describes the fields in the Power Supplies table.

Table 3-11 Power Supply Table Field Descriptions

Field	Description
PS ID	Numeric identifier of the power supply. For more information about the power supplies in your device, see the hardware installation guide for your server switch.
Type	Type of power (AC or DC).
Admin Status	Displays up if you have activated your power supply or down (on select chassis) if you have disabled your power supply.

Table 3-11 Power Supply Table Field Descriptions (continued)

Field	Description
Current 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.

Viewing Power Supply Properties

To view the properties of the power supplies on your device, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Power Supplies** branch.

The Power Supplies table appears in the View frame.

Step 3 Click the radio button next to the power supply with properties you want to view.

Step 4 Click **Properties**.

The Power Supply Properties window opens. Table 3-12 describes the fields in the Power Supplies Properties table.

Table 3-12 Power Supply Property Window Field Descriptions

Field	Description
PS ID	Numeric identifier of the power supply. For more information about the power supplies in your device, see the hardware installation guide for your server switch.
Type	Type of power (AC or DC).
Current 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 Num	Product serial number of the power supply.
PCA Serial Num	PCA serial number of the power supply.
PCA Assembly Num	PCA assembly number of the power supply.
FRU Num	FRU number of the power supply.
Product Version ID	Version of the power supply.

Viewing Fan Status

These topics describe how to view the fan status:

- Viewing Fan Summary Information, page 3-17
- Viewing Fan Properties, page 3-17

Viewing Fan Summary Information

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

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Fans** branch.

The Fans table appears in the View frame. Table 3-13 describes the fields in the Fans table.

Table 3-13 Fan Table Field Descriptions

Field	Description
Fan ID	Numeric identifier of the fan or blower module. For more information, see the hardware installation guide for your server switch.
Current Status	Displays up if the fan functions properly; otherwise, displays down.
Speed (%)	Speed of the fan in percentage of maximum speed.

Viewing Fan Properties

To view the properties of the fans on your device, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Fans** branch.

The Fans table appears in the View frame.

Step 3 Click the radio button next to the fan with properties you want to view.

Step 4 Click **Properties**.

The Fan Properties window opens in the View frame. Table 3-14 describes the fields in the Fan Properties table.

Table 3-14 Fan Properties Window Field Descriptions

Field	Description
Fan ID	Numeric identifier of the fan. For more detail, see the fan documentation.
Current Status	Displays up if the fan functions properly; otherwise, displays down.

Table 3-14 Fan Properties Window Field Descriptions (continued)

Field	Description
Speed	Speed of the fan in the percentage of maximum speed.
Product Serial Num	Product serial number of the fan.
PCA Serial Num	PCA serial number of the fan.
PCA Assembly Num	PCA assembly number of the fan.
FRU Num	FRU number of the fan.
Product Version ID	The ID number of the version of the fan.

Viewing Temperature Sensor Status

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

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Sensors** branch.

The Sensors table appears in the View frame. Table 3-15 describes the fields in the Sensors table.

Table 3-15 Sensors Table Field Descriptions

Field	Description
Slot ID	Numeric identifier of the slot in which the temperature sensor resides. For more information on the slots in your device, see your hardware documentation.
Sensor ID	Numeric identifier of the temperature sensor.
Current Status	Displays up for functional sensors and down for faulty sensors.
Operational Code (Oper Code)	Operational code of the sensor. This field displays normal, tempAlert, currAlert, or voltAlert.
Current Temp (select chassis)	Current temperature of the chassis.
Alarm Temp (select chassis)	Chassis temperature that triggers an alarm.
Shutdown Temp (select chassis)	Chassis temperature that triggers a shutdown.

Viewing the Backplane Information

To view backplane information, follow these steps:

Note This feature is not available on all hardware platforms.

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Select the **Backplane** branch.

The Backplane display appears in the View frame. Table 3-16 describes the fields in this display.

Table 3-16 Backplane Display Field Descriptions

Field	Description
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 Num	Field-replaceable unit (FRU) number.
Chassis ID	GUID of the chassis.
Base MAC Address	24-bit base MAC address of this chassis.
Chassis GUID	GUID of the chassis.
Product Version ID	Version of the backplane.

Viewing Management Ports on a Chassis

To view the configurations of management ports on your device, follow these steps:

Step 1 Expand **Chassis** in the Tree frame.

Step 2 Expand **Management Ports** in the Tree frame.

Step 3 Expand either the **Serial**, **Ethernet**, or **InfiniBand** branch to view the attributes of that management port. See Table 3-17, Table 3-18, and Table 3-19.

Table 3-17 describes the fields in the Serial Management Ports display.

Table 3-17 Serial Management Ports Display Field Descriptions

Field	Description
Baud Rate	Transmission speed to which you must configure your serial connection.
Data Bits	Data bits value to which you must configure your serial connection.
Stop Bits	Stop bits setting to which you must configure your serial connection.
Parity	Parity setting to which you must configure your serial connection.

Table 3-18 describes the fields in the Ethernet Management Ports display.

Table 3-18 Ethernet Management Ports Display Field Descriptions

Field	Description
MAC Address	Media access control (MAC) address of the Ethernet Management Port.
Enable Auto Negotiation	Displays true if you have enabled auto-negotiation and false if you have disabled auto-negotiation.
Administrative Port Status	Displays down if you have shut down the port and up if you brought up the port.
Current Port Status	Displays up if the port runs successfully and down if the port cannot run traffic for physical, logical, or administrative reasons.
IP Address	IP address of the Ethernet Management port.
Net Mask	Subnet mask of the Ethernet Management port.
Gateway	Default IP gateway of the Ethernet Management port.
Address Option	Configured Management Port address option.

Table 3-19 describes the fields in the InfiniBand Management Ports display.

Table 3-19 InfiniBand Management Ports Display Field Descriptions

Field	Description
Administrative Port Status	Displays down if you have shut down the port and up if you brought up the port.
Current Port Status	Displays up if the port runs successfully and down if the port cannot run traffic for physical, logical, or administrative reasons.
IP Address	IP address of the InfiniBand Management port.
Net Mask	Subnet mask of the InfiniBand Management port.
Gateway	Default IP gateway of the InfiniBand Management port.
Address Option	Address option of the InfiniBand management port.
MTU	Maximum transmission unit of the InfiniBand management port.
PKey	Partition used by the InfiniBand management port. See the "Setting the Partition for the InfiniBand Management Port" section on page 3-21.

Setting the Partition for the InfiniBand Management Port

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 change the inband IPoIB management partition, follow these steps:

Step 1 Expand **Chassis** in the Tree frame, and the expand **Management Ports**.

Step 2 Select **InfiniBand**.

The InfiniBand Management Ports window appears.

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

Step 4 Click **Apply**.

CHAPTER 4

Maintenance Tasks

These topics describe the Chassis Manager maintenance tasks:

- Configuring Basic System Information, page 4-1
- Configuring System Global Settings, page 4-3
- Configuring Date and Time Properties, page 4-4
- Configuring the Local Time Zone and Daylight Savings Time, page 4-5
- Viewing or Deleting Files in the File System, page 4-6
- Installing Software Images, page 4-8
- Importing Configuration Files and Image Files with FTP or SCP, page 4-8
- Exporting Configuration Files and Log Files with FTP or SCP, page 4-9
- Customizing the Boot Configuration, page 4-9
- Deleting or Overwriting the Startup Configuration, page 4-10
- Backing Up the Running Configuration File, page 4-10
- Saving a Configuration File, page 4-11
- Rebooting the Device, page 4-11
- Configuring Basic Services, page 4-11
- Viewing and Managing RADIUS Servers, page 4-15
- Viewing and Managing TACACS Servers, page 4-18
- Viewing Authentication Failures, page 4-21
- Viewing Diagnostic Test Results, page 4-22

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 basic system information:

- Viewing System Information, page 4-2
- Naming Your InfiniBand Switch, page 4-2
- Defining a Device Location, page 4-3
- Defining a Cisco TAC Resource, page 4-3

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.

Viewing System Information

To view basic system information, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame. Table 4-1 describes the fields in this table.

Table 4-1 System Information 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 ID (select chassis)	No longer used.
System Sync State	Synchronization state between the primary controller card and the hot standby controller card. (Cisco SFS 7008 and Cisco SFS 7008P Server Switches only.)

Naming Your InfiniBand Switch

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the System Name field, type the name that you want to assign to the device, and then click **Apply**.

Defining a Device Location

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the Location field, type the name location of your device, and then click **Apply**.

Defining a Cisco TAC Resource

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Information** branch.

The System Information display appears in the View frame.

Step 3 In the Support Contact field, type the e-mail address of Cisco TAC, and then click **Apply**.

Configuring System Global Settings

Global configuration includes the system operating mode and the InfiniBand counter reset.

These topics describe how to configure system global settings:

- Configuring System Operation Mode, page 4-3
- Enabling or Disabling InfiniBand Counter Reset, page 4-4

Configuring System Operation Mode

To configure your server switch to deny changes to SRP configuration and preserve VFrame-authorized configurations, set the system operating mode to VFrame Managed. To change the system operation mode, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Global Settings** branch.

The System Global Settings display appears in the View frame.

Step 3 In the System Operation Mode field, choose either the **Normal** or **VFrame Managed** radio button.

Step 4 Click **Apply**.

Enabling or Disabling InfiniBand Counter Reset

Counters are accumulated by the port_agent when performance monitoring is enabled (by default, it is disabled). To enable or disable automatic clearing of the counters by the port_agent, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **System Global Settings** branch.

The System Global Settings display appears in the View frame.

Step 3 In the Enable Counter Reset field, to enable the counter reset function check the **Enable** check box. To disable the counter reset function, uncheck the **Enable** check box.

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 4-4
- Assigning NTP Servers, page 4-5

Configuring the Date and Time

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Time** branch.

The Date and Time Properties display appears in the View frame.

Step 3 In the Date field, enter the date in the *MM*/*DD*/*YY* format.

Step 4 In the Time field, enter the time in *HH*:*MM*:*SS* format, and then click **Apply**.

Assigning NTP Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Time** branch.

The Date and Time Properties display appears in the View frame.

Step 3 In the NTP Server 1 field, enter the IP address of the NTP server that you want your switch to use.

Step 4 (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 5 (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.

Note We recommend that you configure all three NTP servers to maintain time synchronization if a server becomes unreachable.

Configuring the Local Time Zone and Daylight Savings Time

These topics describe how to configure the time zone and daylight savings time on your server switch:

- Setting a Time Zone and Daylight Savings Time, page 4-5
- Resetting the Time Zone and Daylight Savings Time, page 4-6

Note This feature is not available on server switches running the 2.9 version of the operating system.

Setting a Time Zone and Daylight Savings Time

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

Step 1 Expand **Maintenance** in the Tree frame.

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

The Time Zone and Daylight Savings Time Properties window appears.

Step 3 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).

The format for this field is *hh*:*mm*.

For Pacific Standard Time, for example, enter **-08:00**.

Step 4 Leave the Daylight Saving Time section blank if you do not want to configure daylight savings time. Otherwise, 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.

The format for this field is *hh*:*mm*.

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**.

Resetting the Time Zone and Daylight Savings Time

To reset the time zone, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

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

The Time Zone and Daylight Savings Time Properties window appears.

Step 3 In the Time Zone area, delete the information in all fields.

Step 4 In the Daylight Saving Time area, delete the information in all fields.

Step 5 Click **Apply**.

Viewing or Deleting Files in the File System

These topics describe how to view or delete files in the file system:

- Viewing Files in the File System, page 4-7
- Deleting Files in the File System, page 4-7

Viewing Files in the File System

To view device files, such as image files, log files, and configuration files, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame. Table 4-2 describes the fields in this table.

Table 4-2 File Management Table Field Descriptions

Field	Description
Slot ID	Slot of the controller card on which the file resides.
Name	Name of the file.
Type	Type of file. The following appear for selection: • 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 3 (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 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click the radio button next to the file to delete, and then click **Delete**.

A Delete ? confirmation dialog box appears.

Step 4 Click **Yes** in the Delete ? dialog box to delete the file.

Installing Software Images

To install an image file, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Note If you have not already imported the image file to your file system, see the "Importing Configuration Files and Image Files with FTP or SCP" section on page 4-8.

Step 3 Click the radio button next to the image file to install, and then click **Install**.

A dialog box appears to verify that you want to proceed.

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.

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

Step 4 Click **OK** to install the image.

A status bar appears to display the status of the installation.

Importing Configuration Files and Image Files with FTP or SCP

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click **Import**.

The Import File window opens.

Step 4 Choose **FTP** or **SCP** from the Remote Server Type field.

Step 5 Choose a file type (**Image** or **Configuration**) from the File Type drop-down menu.

Step 6 Enter the IP address of the server that holds the file (to be imported) in the Remote IP Address field.

Step 7 Enter your user ID in the Remote User Name field to log into the server.

Step 8 Enter your password in the Remote Password field to log into the server.

Step 9 Enter the directory path and name of the file on the server in the Remote File Path and Name field.

Step 10 Enter the name that the file will take on your chassis in the File Name on System field.

Image files must be saved with an .img extension; otherwise, you will not be able to install these files.

Step 11 Click **Import**.

A status bar appears to display the progress of the file transfer.

Exporting Configuration Files and Log Files with FTP or SCP

Note You cannot export image files.

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **File Management** branch.

The File Management table appears in the View frame.

Step 3 Click the radio button of the file that you want to export.

Step 4 Click **Export**.

The Export File window opens with the name of the file to export in the File Name on System field.

Step 5 Choose **FTP** or **SCP** from the Remote Server Type field.

Step 6 Enter the IP address of the server to which you want to export the file in the Remote IP Address field.

Step 7 Enter your user ID in the Remote User Name field to log into the server.

Step 8 Enter your password in the Remote Password field to log into the server.

Step 9 Enter the directory path and filename for the file on the server in the Remote File Path and Name field.

Step 10 Click **Export**.

A status bar appears to display the progress of the file transfer.

Customizing the Boot Configuration

To customize the boot configuration, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Boot Configuration** branch.

The Boot Configuration display appears in the View frame.

Step 3 (Optional) 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 4 Click **Apply**.

Deleting or Overwriting the Startup Configuration

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Boot Configuration** branch.

The Boot Configuration display appears in the View frame.

Step 3 Click the **Overwrite startup configuration with** radio button, and then choose a configuration from the drop-down menu to replace the current startup configuration file.

Note To overwrite your startup configuration with your running configuration, see the "Backing Up the Running Configuration File" section on page 4-10.

Step 4 (Optional) Click the **Delete startup configuration** radio button to configure your server switch to use the factory-default startup configuration.

Step 5 Click **Apply**.

Backing Up the Running Configuration File

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Backup Configuration** branch.

The Backup Configuration display appears in the View frame.

Step 3 Enter a filename in the Save Configuration As field.

Chassis Manager saves running configurations 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.

Step 4 Click **Save**.

Step 5 (Optional) Click the **File Management** branch to verify that your file appears in the file system.

Saving a Configuration File

To back up your running configuration as your startup configuration (and to the standby controller on your chassis with a dual-controller chassis), follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Save Config** branch.

The Save Config display appears in the View frame.

Step 3 Click **Save Config**.

Rebooting the Device

When you reboot your device, Chassis Manager gives you the option to reboot either with or without saving your configuration. If you choose to reboot but not save, any differences between your running configuration file and startup configuration file are not saved after the reboot.

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Select the **Reboot** branch.

The Reboot display appears in the View frame.

Step 3 To save the system configuration and reboot, click **Save-Reboot**. To reboot without saving the system configuration, click **Reboot-Only**.

Configuring Basic Services

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

- Assigning a DNS Server, page 4-12
- Enabling or Disabling the FTP Access, page 4-12
- Enabling or Disabling the Telnet Access, page 4-12
- Assigning a Syslog Server, page 4-13
- Assigning an Authentication Method, page 4-13
- Configuring HTTP and HTTPS, page 4-15

Assigning a DNS Server

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Server 1 field, enter the IP address of the primary DNS server that you want to use.

Step 5 (Optional) In the Server 2 field, enter the IP address of the DNS server to use if your device cannot access the primary DNS server.

Step 6 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 FTP transfers to and from your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the FTP Server field, check to enable or uncheck to disable the **Enable** check box, and then click **Apply**.

Enabling or Disabling the Telnet Access

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Telnet Server field, check (enable) or uncheck (disable) the **Enable** check box, 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 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame. You can use either one or two servers.

Step 4 In the Remote Syslog Server field, enter the IP address of the remote server(s). The sever switch will send messages to this device.

Step 5 Click **Apply**.

Assigning an Authentication Method

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **General** branch.

The System Services display appears in the View frame.

Step 4 In the Authentication Method field (under the Radius heading), click a radio button to choose a method, and then click **Apply**. Table 4-3 describes the radio buttons that you can choose.

Table 4-3 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.

Configuring HTTP and HTTPS

To configure HTTP and HTTPS services, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **HTTP** branch.

The System HTTP display appears in the View frame.

Step 4 (Optional) Check or uncheck the **Enable** check box in the Polling field to enable or disable automatic polling.

Step 5 (Optional) Click a radio button in the Secure Cert Common Name field of the identifier that you want to use for security certification.

Step 6 Click **Apply**.

Viewing and Managing RADIUS Servers

These topics describe how to view and manage RADIUS servers:

- Viewing RADIUS Servers, page 4-15
- Viewing and Configuring RADIUS Server Properties, page 4-16
- Adding RADIUS Servers, page 4-17
- Deleting RADIUS Servers, page 4-18

Viewing RADIUS Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers display appears in the View frame. Table 4-4 describes the fields in the Radius Servers table.

Table 4-4 Radius Servers Table Field Descriptions

Field	Description
Address	Displays the IP address of the RADIUS server.
Priority	Sequence number designating the order in which the authentication process accesses Radius servers. Priority is assigned in the order in which you configure Radius servers.
UDP Port	UDP authentication port of the RADIUS server.

Table 4-4 Radius Servers Table Field Descriptions (continued)

Field	Description
Encryption Key	Authentication key that the client and RADIUS server use.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username altogether.

Viewing and Configuring RADIUS Server Properties

To view and configure RADIUS servers to authenticate CLI logins, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server whose properties you want to view or configure, and then click **Properties**.

The Radius Server Properties window opens. Table 4-5 describes the fields in the Radius Server Properties window.

Table 4-5 Radius Server Properties Window Fields

Field	Description
Address field	Displays the IP address of the RADIUS server.
UDP Port field	UDP 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 of integer values that this field supports.
Encryption Key	Authentication key that the client and RADIUS server use. 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 of integer values that this field supports.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails. 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 of integer values that this field supports.

Table 4-5 Radius Server Properties Window Fields (continued)

Field	Description
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username. 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 of integer values that this field supports.
Priority	Server priority for use.
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 configure a new RADIUS server on your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click **Add**.

The Add 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 5 In the Address field, enter the IP address of the server.

Step 6 (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 7 (Optional) Enter an encryption key in the Encryption Key field.

Step 8 (Optional) Edit the Timeout field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 (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 10 Click **Apply**.

Deleting RADIUS Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Radius Servers** branch.

The Radius Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server that you want to delete.

Note Chassis Manager will not prompt you to be sure that you want to delete this server.

Step 5 Click **Delete**.

Viewing and Managing TACACS Servers

These topics describe how to view and manage TACACS servers:

- Viewing TACACS Servers, page 4-18
- Viewing and Configuring TACACS Server Properties, page 4-19
- Adding TACACS Servers, page 4-20
- Deleting TACACS Servers, page 4-21

Viewing TACACS Servers

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers display appears in the View frame. Table 4-6 describes the fields in the Tacacs Servers table.

Table 4-6 Tacacs Servers Table Field Descriptions

Field	Description
Address	Displays the IP address of the TACACS server.
Priority	Server priority for use.
UDP Port	UDP authentication port of the TACACS server.
Encryption Key	Authentication key that the client and TACACS server use.

Table 4-6 Tacacs Servers Table Field Descriptions (continued)

Field	Description
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username.

Viewing and Configuring TACACS Server Properties

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

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server whose properties you want to view or configure, and then click **Properties**.

The Tacacs Server Properties window opens. Table 4-7 describes the fields in the Tacacs Server Properties window.

Table 4-7 Tacacs Server Properties Window Fields

Fields	Description
Address	Displays the IP address of the TACACS server.
Priority	Server priority for use.
UDP Port	UDP 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.
Encryption Key	Authentication key that the client and TACACS server use. 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 of integer values that this field supports.
Timeout	Amount of time, in seconds, in which the server must authenticate a login before the login fails. 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 of integer values that this field supports.

Table 4-7 Tacacs Server Properties Window Fields (continued)

Fields	Description
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username. 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 TACACS Servers

To configure a new TACACS server on your device, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click **Add**.

The Add Tacacs 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 5 In the Address field, enter the IP address of the server.

Step 6 (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 7 (Optional) Enter an encryption key in the Encryption Key field.

Step 8 (Optional) Edit the Timeout field. The numbers to the right of the field indicate the range of integer values that this field supports.

Step 9 (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 10 Click **Apply**.

Deleting TACACS Servers

To remove a TACACS server from your configuration, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Tacacs Servers** branch.

The Tacacs Servers table appears in the View frame.

Step 4 Click the radio button to the left of the server that you want to delete.

Step 5 Click **Delete**.

Viewing Authentication Failures

To view a log of authentication failures for your server switch, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Services** in the Tree frame.

Step 3 Select the **Authentication Failures** branch.

The Authentication Failures display appears in the View frame. Table 4-8 describes the fields in this display.

Table 4-8 Authentication Failures Field Descriptions

Field	Description
CLI Access Violation Count	Cumulative number of failed CLI logins since the server switch booted.
CLI Last Violation Time	Time of the most recent failed CLI login.
SNMP Access Violation Count	Cumulative number of failed SNMP logins since the server switch booted.
SNMP Last Violation Time	Time of the most recent failed SNMP login.
HTTP Access Violation Count	Cumulative number of failed HTTP logins since the server switch booted.
HTTP Last Violation Time	Time of the most recent failed HTTP login.

Viewing Diagnostic Test Results

Available test results vary by hardware platform.

These topics describe how to view diagnostic test results:

- Viewing Card POST Test Results, page 4-22
- Viewing Fan POST Test Results, page 4-23
- Viewing Power Supply POST Test Results, page 4-23
- Viewing Card FRU Errors, page 4-24
- Viewing Fan FRU Errors, page 4-24
- Viewing Power Supply FRU Errors, page 4-25

Viewing Card POST Test Results

To view power-on self-test results for a card, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-9 describes the fields in the table.

Table 4-9 Card POST Test Status Field Descriptions

Field	Description
Card	Card on which the power-on self-test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Fan POST Test Results

To view power-on self-test results for a fan, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-10 describes the fields in the table.

Table 4-10 Fan POST Test Status Field Descriptions

Field	Description
Fan	Fan on which the power-on self-test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Power Supply POST Test Results

To view power-on self-test results for a power supply, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **POST** branch.

The POST Status table appears in the View frame. Table 4-11 describes the fields in the table.

Table 4-11 Power Supply POST Test Status Field Descriptions

Field	Description
Power Supply	Power supply on which the POST test ran.
Post Status	Status of the test.
Error Code	Applicable error codes that resulted from the test.

Viewing Card FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view card FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Card portion of the display.

Table 4-12 Card FRU Field Descriptions

Field	Description
Card	Slot number of the card.
Error Code	Shows the last hardware error (if any) detected on this card. The information provided in this field is read from the vital product data of the device.

Viewing Fan FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view fan FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Fan portion of the display.

Table 4-13 Fan FRU Field Descriptions

Field	Description
Fan	Fan number.
Error Code	Shows the last hardware error (if any) detected on this fan. The information provided in this field is read from the vital product data of the device.

Viewing Power Supply FRU Errors

Note This procedure displays runtime errors that are not caught by POST. POST errors are also displayed using this procedure.

To view power supply FRU errors, follow these steps:

Step 1 Expand **Maintenance** in the Tree frame.

Step 2 Expand **Diagnostics** in the Tree frame.

Step 3 Select the **Fru Error** branch.

The Fru Error display appears in the View frame. Table 4-12 describes the fields shown in the Card portion of the display.

Table 4-14 Power Supply FRU Field Descriptions

Field	Description
Power Supply	Power supply number.
Error Code	Shows the last hardware error (if any) detected on this power supply. The information provided in this field is read from the vital product data of the device.

CHAPTER 5

InfiniBand Tasks

This chapter describes the Chassis Manager InfiniBand tasks and contains these sections:

- Viewing and Managing Subnet Managers, page 5-1
- Viewing InfiniBand Services, page 5-6
- Viewing InfiniBand Nodes, page 5-7
- Viewing InfiniBand Ports, page 5-10
- Viewing Neighboring InfiniBand Devices, page 5-16
- Viewing IOUs, page 5-18
- Viewing IOCs, page 5-19
- Viewing IOC Services, page 5-21

Viewing and Managing Subnet Managers

These topics describe how to view and manage subnet managers:

- Viewing Subnet Managers, page 5-1
- Viewing Subnet Manager Properties, page 5-2
- Adding a Subnet Manager, page 5-4
- Deleting a Subnet Manager, page 5-4
- Configuring Subnet Manager Properties, page 5-4

Viewing Subnet Managers

The subnet managers display in Chassis Manager provides an abridged version of the output of the **show ib sm** CLI command. To view the subnet managers in your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Subnet Managers** branch.

The Subnet Managers table appears in the View frame. Table 5-1 describes the fields in the Subnet Managers table.

Table 5-1 Subnet Managers Table Field Descriptions

Field	Description
Subnet Prefix	64-bit value that identifies the InfiniBand subnet.
GUID	GUID of the server switch.
Oper-Status	Displays the operating status (oper-status) of the SM.

Viewing Subnet Manager Properties

To view Subnet Manager properties, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Subnet Managers** branch.

The Subnet Managers table appears in the View frame.

Step 3 Click the radio button next to the subnet manager that you want to view, and then click **Properties**.

The Subnet Manager Properties window opens. Table 5-2 describes the fields in this window.

Table 5-2 Subnet Manager Properties Window Fields

Field	Description
Subnet Prefix	Displays the subnet prefix of the subnet manager.
GUID	Displays the GUID of the networking device on which the subnet manager runs.
Status	Status of the subnet manager. It may appear as master, standby, inactive, or discovery.
Activity Count	Activity counter that increments each time that the subnet manager sends a subnet management packet (SMP) or performs other management activities.
SM Key	Subnet Manager Verification Key is used by the master subnet manager to authenticate other master and standby subnet managers. Subnet Manager Key is also used in SA query handling to ensure a request is from a trusted source. Note that Subnet Manager Key is not enforced in release 2.9.0.
Priority	Priority of the subnet manager relative to other subnet managers in the InfiniBand network. The higher the number, the greater the priority.
Sweep Interval	Specifies how frequently the subnet manager queries the InfiniBand fabric for network changes.
Response Timeout	Timeout interval in milliseconds that the subnet manager waits before resending a management datagram (MAD).

Table 5-2 Subnet Manager Properties Window Fields (continued)

Field	Description
Master Poll Interval	Interval at which a standby subnet manager polls the master to see if it is still running.
Master Poll Retries	Number of unanswered polls that cause the standby to identify the master as dead.
Max Active SMs	Maximum number of standby subnet managers that the 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	Life time of a packet inside a server switch.
Switch Link HoQ Life	Life time of a packet at the head-of-queue of a switch port.
CA Link HoQ Life	Life time of a packet at the head-of-queue of the host port.
Maximum Hop Count	Maximum number of hops considered by the subnet manager when calculating routes in a subnet. Range is from 0 to 64. The default value is 64. A value of 0 indicates that the subnet manager has been configured to calculate and use the lowest possible value that ensures connectivity between all endpoints.
MAD Retries	Number of times the subnet manager resends a MAD after not receiving a response. The default value is 5.
NodeTimeout	Minimum amount of time in seconds that a HCA may be unresponsive before the subnet manager removes it from the InfiniBand fabric. The default value is 10 seconds.
Wait Report Response	Whether or not the subnet manager waits to receive ReportResponse MADs in response to the Report MADs that it forwards. This value is a boolean value. If 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 ReportResponse MAD is received or the maximum number of Report MADs have been sent. The default value is false.
SA MAD Queue Depth	Size of the internal queue of the SA for receiving MADs. The default value is 256.

Adding a Subnet Manager

To add a subnet manager, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Subnet Managers** branch.

The Subnet Managers table appears in the View frame.

Step 3 Click **Add**.

The Add Subnet Manager window opens.

Step 4 Enter a subnet prefix in the Subnet Prefix field. The default value is fe:80:00:00:00:00:00:00.

Step 5 Assign a priority value (integer) between 0 and 15 in the Priority field. The higher the integer, the higher the priority. The default value is 0.

Step 6 (Optional) Enter a key in the Subnet Manager Key field. The default value is 00:00:00:00:00:00:00:00.

Step 7 Click **Apply**.

Deleting a Subnet Manager

To delete a subnet manager, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Subnet Managers** branch.

The Subnet Managers table appears in the View frame.

Step 3 Click the radio button next to the subnet manager that you want to delete, and then click **Delete**.

Step 4 Click **OK**.

Configuring Subnet Manager Properties

Caution Only advanced users should attempt to fine tune subnet manager properties. Default values are adequate for most purposes,

To configure subnet manager properties, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Subnet Managers** branch.

The Subnet Managers table appears in the View frame.

Step 3 Click the radio button next to the subnet manager that you want to view, and then click **Properties**.

The Subnet Manager Properties window opens.

Step 4 Enter an integer (0 – 15) in the Priority field to configure the priority of the subnet manager; the higher the number, the greater the priority.

Step 5 Enter an integer (1 – 268435455) in the Sweep Interval field to configure the sweep interval, in seconds, of the subnet manager.

Step 6 Enter an integer (100 – 5000) in the Response Timeout field to configure how long the subnet manager waits, in milliseconds, for a response from a connection before it resends a MAD. The default value is 200 milliseconds.

Step 7 Enter an integer (1 – 60) in the Master Poll Interval field to configure the interval, in seconds, at which the slave subnet manager polls the master to see if the master still runs.

Step 8 Enter an integer (1 – 10) in the Master Poll Retries field to configure the number of unanswered polls that cause the standby to identify the master as dead.

Step 9 Enter an integer value (0 – 9999) in the Max Active Subnet Managers field to configure the maximum number of standby subnet managers that the master supports. This value defaults to 0, which indicates unlimited subnet managers.

Step 10 Enter an integer value (0 – 7) in the LID Mask Control field to configure LID mask control on your subnet manager.

Step 11 Enter an integer value between 0 and 20 in the Switch Life Time field.

Step 12 Enter an integer value between 0 and 20 in the Switch Link HoQ Life field.

Step 13 Enter an integer (0 – 100) in the MadRetries field to configure the number of times the subnet manager resends a MAD after not receiving a response. The default value is 5.

Step 14 Enter an integer (1 – 2000) in the NodeTimeout field to configure the minimum amount of time in seconds that a HCA may be unresponsive before the subnet manager removes it from the InfiniBand fabric. The default value is 10 seconds.

Step 15 Check or uncheck the **WaitReportResponse** check box to configure whether or not the subnet manager waits to receive ReportResponse MADs in response to the Report MADs that it forwards.

This is a boolean value. If 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 ReportResponse MAD is received or the maximum number of Report MADs have been sent. The default value is False.

Step 16 Enter an integer (256 – 1024) in the SaMadQueueDepth field to configure the size of the internal queue of the SA for receiving MADs. The default value is 256.

Step 17 Click **Apply** to apply your change(s) to your server switch.

Viewing InfiniBand Services

These topics describe how to view InfiniBand services:

- Viewing InfiniBand Services Summary Information, page 5-6
- Viewing InfiniBand Service Properties, page 5-6

Viewing InfiniBand Services Summary Information

Subnet services provide various features for your InfiniBand fabric, such as the ability to run particular protocols. To view the subnet services on your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Select the **Services** branch.

The Services table appears in the View frame. Table 5-3 lists and describes the fields in the Services table.

Table 5-3 Services Table Fields

Field	Description
Name	Name of the subnet service.
Subnet Prefix	Subnet prefix of the subnet service.
Service ID	ID of the service.
Service GID	GID of the port that offers the service.
PKey	Partition key used to contact the service.

Viewing InfiniBand Service Properties

To view InfiniBand service properties, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame, and select the **Services** branch.

The Services table appears in the View frame.

Step 2 Click the radio button next to the service whose properties you want to view, and then click **Properties**.

The InfiniBand Service Properties window opens. Table 5-4 lists and describes the fields in this window.

Table 5-4 InfiniBand Service Properties Window Fields

Field	Description
Subnet Prefix	Subnet prefix of the service.
Service ID	ID of the service.
Service GID	GID of the service.

Table 5-4 InfiniBand Service Properties Window Fields (continued)

Field	Description
PKey	Partition key of the service.
Lease	Lease period of the service.
Key	Key of the service.
Name	Name of the service.
Data (8 bit)	8-bit service data.
Data (16 bit)	16-bit service data.
Data (32 bit)	32-bit service data.
Data (64 bit)	64-bit service data.

Viewing InfiniBand Nodes

These topics describe how to view InfiniBand node information:

- Viewing InfiniBand Node Summary Information, page 5-7
- Viewing Node Properties, page 5-8
- Viewing Node Ports, page 5-10
- Viewing Node Neighbors, page 5-10

Viewing InfiniBand Node Summary Information

Both InfiniBand switches and InfiniBand hosts qualify as InfiniBand nodes. To view the nodes in your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the InfiniBand frame, and select the **Nodes** branch.

The Nodes table appears in the View frame. Table 5-5 lists and describes the fields in the Nodes table.

Table 5-5 Nodes Table Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the node. The prefix of the node matches the prefix of the Subnet Manager that manages the node.
Node GUID	GUID of the switch or host.
Description	Description of the node.
Type	Identifies the hardware type of the node.

Viewing Node Properties

To view the properties of a switch or host in your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the InfiniBand frame.

Step 3 Select the **Nodes** branch.

The Nodes table appears in the View frame.

Step 4 Click the radio button next to the node that you want to view, and then click **Properties**.

The Topology Node Properties window opens. Table 5-6 describes the Topology Node Properties fields in the window.

Table 5-6 Topology Node Properties Window Field Descriptions

Field	Description
Subnet Prefix	64-bit value that identifies the InfiniBand subnet to which this node belongs.
Node GUID	GUID of this 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 1.0*, 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.
Type	Type of node being managed. The value is channel adapter, switch, router, or error. An error entry indicates an unknown type.
Num Ports	Number of physical ports on this node.
Port GUID	GUID of this port. A port within a node can return the node GUID as its PortGUID if the port is an integral part of the node and is not field-replaceable (not swappable).
Partition Cap	Capacity of entries in the partition table for channel adapter, router, and the switch management port. The value is the same for all ports on the node. This is set to at least 1 for all nodes including switches. This value is fixed and unconfigurable.
Device ID	Manufacturer-assigned device identification.
Revision	Manufacturer-assigned device revision.
Local Port Num	The link port number from which this subnet management packet (SMP) arrived. The value is the same for all ports on the node.
Vendor ID	Device vendor ID. The value is the same for all ports on the node.
Description	Description of the node.
System Image GUID	The system image GUID of this node. All nodes within a particular system (chassis) are assigned the same system image GUID.

Table 5-7 lists and describes the Switch Properties fields in the window.

Table 5-7 Topology Node Properties Window Field Descriptions, Switch Properties

Field	Description
Linear FDB Cap	Maximum number of entries allowed in the linear unicast forwarding table. 0 (zero) indicates that there is no linear forwarding database.
Random FDB Cap	Maximum number of entries allowed in the random unicast forwarding table. 0 (zero) indicates that there is no random forwarding database.
MCast FDB Cap	Maximum number of entries allowed in the multicast forwarding table.
Linear FDB Top	Specifies the top of the linear forwarding table. Packets received with unicast LIDs greater than this value are discarded by the switch. This parameter applies only to switches that implement linear forwarding tables and is ignored by switches that implement random forwarding tables.
Default Port	Specifies the default port to which to forward all the unicast packets from other ports whose destination local identifier (DLID) does not exist in the random forwarding table.
Default Primary MCast Port	Specifies the default port to which to forward all the multicast packets from other ports whose DLID does not exist in the multicast forwarding table.
Default Non-Primary MCast Port	Specifies the port to which to forward all the multicast packets from default-pri-mcast-port whose DLID does not exist in the multicast forwarding table.
Lifetime Value	Specifies the duration a packet can live in the switch. Time units are in milliseconds. See section 18.2.5.4, “Transmitter Queueing,” in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
Switch Port State Change	Indicates a change in port state. The value is either 0 (no change) or 1.
LID Per Port	Number of LID/LMC combinations that may be assigned to a given external port for switches that support the random forwarding table. This value is always 0. 0 indicates that there is one LID per port.
Partition Enforce Cap	Number of entries in this partition enforcement table per physical port. 0 (zero) indicates that partition enforcement is not supported by the switch.
In Enforce Cap	Indicates if the switch is capable of partition enforcement on received packets. The value is true (1) or false.
Out Enforce Cap	Indicates if the switch is capable of partition enforcement on transmitted packets. The value is true (1) or false.
In Filter Raw Packet Cap	Indicates if the switch is capable of raw packet enforcement on received packets. The value is true (1) or false.
Out Filter Raw Packet Cap	Indicates if the switch is capable of raw packet enforcement on transmitted packets. The value is true (1) or false.

Viewing Node Ports

To view the InfiniBand ports on a node in your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the InfiniBand frame.

Step 3 Select the **Nodes** branch.

The Nodes table appears in the View frame.

Step 4 Click the radio button next to the node whose ports you want to view, and then select **Show Ports** from the Show Options drop-down menu.

The InfiniBand Ports display appears in the View frame, but lists only the ports that belong to the node that you selected. For details, see the "Viewing InfiniBand Ports" section on page 5-10 or see Table 5-8.

Viewing Node Neighbors

To view the neighbors of an InfiniBand node on your fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the InfiniBand frame.

Step 3 Select the **Nodes** branch.

The Nodes table appears in the View frame.

Step 4 Click the radio button next to the node whose neighbors you want to view, and then select **Show Neighbors** from the Show Options pull-down menu.

The InfiniBand Neighbors display appears in the View frame but lists only the neighbors of the node that you selected. For details, see the "Viewing Neighboring InfiniBand Devices" section on page 5-16 or see Table 5-10.

Viewing InfiniBand Ports

Thee topics describe how to view InfiniBand port information:

- Viewing All InfiniBand Ports, page 5-11
- Viewing InfiniBand Port Properties, page 5-11

Viewing All InfiniBand Ports

To view the InfiniBand ports on your InfiniBand fabric, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the Tree frame.

Step 3 Select the **Ports** branch in the Tree frame.

The InfiniBand Ports table appears in the View frame. Table 5-8 describes the fields in the InfiniBand Ports table.

Table 5-8 InfiniBand Ports Table Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the device on which the port resides.
Node GUID	GUID of the node on which the port resides.
Port	Numeric identifier of the port.
LID	Local identifier of the port.
State	Displays the port state as active, armed, noStateChange, initialize, reserved, or down.
Link Width Active	Speed of the connection to this port. The value is 1x, 4x, or 12x.

Viewing InfiniBand Port Properties

To view the properties of an InfiniBand port, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the Tree frame.

Step 3 Select the **Ports** branch in the Tree frame.

The InfiniBand Ports table appears in the View frame.

Step 4 Click the radio button next to the port whose properties you want to view, and then click **Properties**.

The Topology Port Properties window opens. Table 5-9 describes the fields in the Topology Port Properties window.

Table 5-9 Topology Port Properties Window Field Descriptions

Field	Description
Subnet Prefix	64-bit value that identifies the InfiniBand subnet to which this port belongs.
Node GUID	64-bit GUID of the node to which this port belongs.
Port	Port number (integer) of the node.

Table 5-9 Topology Port Properties Window Field Descriptions (continued)

Field	Description
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 1.0*, for more information.
GID Prefix	64-bit GID prefix for this port. This prefix is assigned by the subnet manager, based upon port routes and the rules for local identifiers. See section 4.1.3, "Local Identifiers," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
LID	16-bit identifier of the port.
Master SM LID	16-bit identifier 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 1.0*, for more information. This field does not currently apply to your device.
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 nonzero 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 is never to expire. See *InfiniBand Architecture*, Vol. 1, Release 1.0, section 14.2.4, "Management Key," for more information.

Table 5-9 Topology Port Properties Window 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 is one of the following: • 1x, • 1x, 4x • 1x, 4x, 8x • 1x, 4x, 12x, • 1x, 4x, 8x, 12x • reserved
Link Width Active	Active link width. Used with Active Link Speed to determine the link rate between two nodes. The value is 1x, 4x, or 12x.
Supported Link Speed	Supported link speed. The value appears as one of the following: • sdr • sdr, ddr
State	A higher form of addressing than Physical State, this state determines that the nodes can actually communicate and indicates the state transition that has occurred. A transition is a port change from down to initialize, initialize to down, armed to down, or active to down as a result of link state machine logic. Changes to the port state resulting from SubnSet have no affect on this parameter value. The value is noStateChange, down, initialize, armed, or active.
Physical State	Indicates the physical state of the port. This is used to determine that electricity is flowing between nodes and they can perform a handshake. The value is noStateChange, sleeping, polling, disabled, portConfigurationTraining, linkup, or linkErrorRecovery. The default state upon power-up is polling.

Table 5-9 Topology Port Properties Window Field Descriptions (continued)

Field	Description
Link Down Def State	Default LinkDown state to return to. The value is noStateChange, sleeping, or polling. See section 5.5.2, "Status Outputs (MAD GET)," in *InfiniBand Architecture, Vol. 2, Release 1.0*, for more information.
MKey Protocol 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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
LID Mask	Local-identifier mask control (LMC) for multipath support. A LMC is assigned to 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 is allowed on this port. See sections 3.5.10, "Addressing," and 4.1.3, "Local Identifiers," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
Active Link Speed	Speed of an active link: sdr or 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 is mtu256, mtu512, mtu1024, mtu2048, or mtu4096.
Master SM SL	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 is vl0, vl0ToVl1, vl0ToVl3, vl0ToVl7, or vl0ToVl14. 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 (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 is determined by checking the VL Arb High Cap on the other side of the link and then negotiating downward.
VL Arb High Cap	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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
Vl Arb 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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.

Table 5-9 Topology Port Properties Window Field Descriptions (continued)

Field	Description
MTU Cap	Used 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 is mtu256, mtu512, mtu1024, mtu2048, or mtu4096.
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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for a description of HLL.
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 is vl0, vl0ToVl1, vl0ToVl3, vl0ToVl7, or vl0ToVl14.
In Partition Enforcement	Boolean value that indicates whether or not to support optional partition enforcement for the packets received by this port. There is no default value.
Out Partition Enforcement	Boolean value that indicates whether or not to support optional partition enforcement for the packets transmitted by this port. There is no default value.
In Filter Raw Packet Enforcement	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets received by this port. There is no default value.
Out Filter Raw Packet Enforcement	Boolean value that indicates whether or not to support optional raw packet enforcement for the raw packets transmitted by this port. There is no default value.
MKey Violation	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," in I*nfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
PKey Violation	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)," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
QKey Violation	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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, 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," in I*nfiniBand Architecture, Vol. 1, Release 1.0*, for more information.

Table 5-9 Topology Port Properties Window Field Descriptions (continued)

Field	Description
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 which traps can be sent from this port. Delay is affected by switch configuration. This parameter, along with Response Time, is used to determine the interval to wait for a response to a request before taking other action. Duration is calculated as (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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
Local Physical 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," in *InfiniBand Architecture, Vol. 1, Release 1.0*, for more information.
Local Overrun Error	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 Neighboring InfiniBand Devices

These topics describe how to view information about neighboring InfiniBand devices:

- Viewing All Neighboring InfiniBand Devices, page 5-16
- Viewing InfiniBand Neighbor Properties, page 5-17

Viewing All Neighboring InfiniBand Devices

To view the InfiniBand devices that directly connect to your device, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the Tree frame.

Step 3 Select the **Neighbors** branch in the Tree frame.

The InfiniBand Neighbors table appears in the View frame. Table 5-10 lists and describes the fields in this table.

Table 5-10 InfiniBand Neighbors Table Field Descriptions

Field	Description
Subnet Prefix	64-bit value that identifies the InfiniBand subnet to which this neighbor node belongs.
Local Node GUID	64-bit GUID of the InfiniBand node.
Local Port ID	Port ID of the InfiniBand node. The value is an integer between 0 and 255.
Remote Node GUID	64-bit Guid of the neighboring InfiniBand node to which the local node is linked.
Remote Port ID	Port ID of the neighboring InfiniBand node to which the local node is linked. The value is an integer between 0 and 255.

Viewing InfiniBand Neighbor Properties

To view InfiniBand neighbor properties, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Topology** in the Tree frame.

Step 3 Select the **Neighbors** branch.

The InfiniBand Neighbors table appears in the View frame.

Step 4 Click the radio button next to the neighbor whose properties you want to view, and then click **Properties**.

The Topology Neighbor Properties window opens. Table 5-11 describes the fields in this window.

Table 5-11 Topology Neighbor Properties Window Field Descriptions

Field	Description
Subnet Prefix	Subnet prefix of the neighbor node.
Local Node GUID	GUID of the neighbor that you selected.
Local Port ID	Local port on the neighbor that you selected that connects to your server switch.
Local Node Type	Node type of the neighbor node.
Remote Node GUID	GUID of the physical switch within your server switch that connects to the neighbor node.
Remote Port ID	Port on the physical switch within your server switch that connects to the neighbor node.
Remote Node Type	Node type of the physical switch within your server switch that connects to the neighbor node.

Table 5-11 Topology Neighbor Properties Window Field Descriptions (continued)

Field	Description
Link State	State of the connection between the neighbor and the switch within your server switch.
Link Width Active	Bandwidth of the connection between the neighbor and the switch within your server switch.

Viewing IOUs

To view the I/O Units (IOUs) on your device, follow these steps:

Note This feature is not available on all hardware platforms. IOUs and IOCs can be viewed only on chassis that support I/O modules (gateways).

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Device Management** in the Tree frame.

Step 3 Select the **IOU** branch.

The IOU display appears in the View frame. Table 5-12 describes the fields in this display.

Table 5-12 IOU Display Field Descriptions

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	Indicates that diagnostics can (1) or cannot (0) provide IOC details.
Option ROM	Indicates the presence or absence of Option ROM.
Controller List	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

These topics describe viewing information about IOCs:

- Viewing All IOCs, page 5-19
- Viewing IOC Properties, page 5-19

Viewing All IOCs

To view the I/O controllers (IOCs) on your device, follow these steps:

Note This feature is not available on all hardware platforms. IOUs and IOCs can be viewed only on chassis that support I/O modules (gateways).

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Device Management** in the Tree frame.

Step 3 Select the **IOCs** branch.

The IOCs display appears in the View frame. Table 5-13 describes the fields in this display.

Table 5-13 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.
IO Class	I/O class that the IOC supports.
Protocol	Standard protocol definition that the IOC supports.

Viewing IOC Properties

To view the properties of the I/O controllers (IOCs) on your device, follow these steps:

Note This feature is not available on all hardware platforms.

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Device Management** in the Tree frame.

Step 3 Select the **IOCs** branch.

The IOCs display appears in the View frame.

Step 4 Click the radio button next to the IOC that you want to view, and then click **Properties**.

The IOC Properties window opens. Table 5-14 describes the fields in this window.

Table 5-14 IOC Properties Window 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.
IO Class	I/O class that the IOC supports.
IO Subclass	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 Mask	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

These topics describe how to view information about IOC services:

- Viewing All IOC Services, page 5-21
- Viewing Properties of IOC Services, page 5-21

Viewing All IOC Services

To view the IOC services on your device, follow these steps:

Note This feature is not available on all hardware platforms.

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Device Management** in the Tree frame.

Step 3 Select the **IOC Services** branch in the Tree frame.

The IOC Services table appears in the View frame. Table 5-15 lists and describes the fields in this table.

Table 5-15 IOC Services Table Field Descriptions

Field	Description
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.

Viewing Properties of IOC Services

Note This feature is not available on all hardware platforms.

To view the properties of IOC services on your device, follow these steps:

Step 1 Expand **InfiniBand** in the Tree frame.

Step 2 Expand **Device Management** in the Tree frame.

Step 3 Select the **IOC Services** branch in the Tree frame.

The IOC Services table appears in the View frame.

Step 4 Click the radio button next to the service whose properties you want to view, and then click **Properties**.

The InfiniBand Service Properties window opens. Table 5-16 describes the fields in this window.

Table 5-16 InfiniBand Service Properties Window Field Descriptions

Field	Description
Subnet Prefix field	Subnet prefix of the service.
Service ID field	Numeric identifier that nodes use to call the service.
Service GID field	Global ID (GID) of the service.
PKey field	Partition key of the service.
Lease field	Lease period of the service.
Key field	Subnet management key of the service.
Name field	ASCII identifier of the service.
Data (8 bit) field	8-bit descriptor of the service.
Data (16 bit) field	16-bit descriptor of the service.
Data (32 bit) field	32-bit descriptor of the service.
Data (64 bit) field	64-bit descriptor of the service.

CHAPTER 6

Ethernet Tasks

These topics describe the Chassis Manager Ethernet tasks:

- Viewing and Managing Bridge Groups, page 6-1
- Viewing and Managing Bridge Subnets, page 6-5
- Viewing and Managing Bridge Forwarding, page 6-6
- Viewing and Managing Redundancy Groups, page 6-8
- Viewing and Managing Trunk Groups, page 6-11

Viewing and Managing Bridge Groups

These topics describe how to view and manage bridge groups:

- Viewing Bridge Groups, page 6-1
- Viewing Bridge Group Properties, page 6-2
- Adding Bridge Groups, page 6-3
- Configuring Bridge Groups, page 6-4
- Deleting Bridge Groups, page 6-5

Viewing Bridge Groups

To view the bridge groups on your server switch, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Groups** branch.

The Bridge Groups table appears in the View frame. Table 6-1 describes the fields in this table.

Table 6-1 Bridge Groups Table Field Descriptions

Field	Description
ID	Bridge group ID number.
Name	Bridge group name.

Table 6-1 Bridge Groups Table Field Descriptions (continued)

Field	Description
Ethernet Port	Trunk group and ports available that the bridge group uses to connect to the Ethernet switch.
IB Port	Internal gateway slot#/port# that is associated with the bridge-group.
IB P_KEY	InfiniBand partition key of the bridge group.
Broadcast Forwarding	Broadcast forwarding configuration of the bridge group.
Gratuitous IGMP	Displays true if gratuitous IGMP is set; otherwise, displays false.

Viewing Bridge Group Properties

To view the properties of a bridge group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Groups** branch.

The Bridge Groups table appears in the View frame.

Step 3 Click the radio button next to the bridge group whose properties you want to view, and then click **Properties**.

The Ethernet Chassis Manager window opens and displays the properties of the bridge group. Table 6-2 describes the fields in this window.

Table 6-2 Ethernet Chassis Manager Window Field Descriptions

Field	Description
ID	ID number of the bridge group.
Name	Name of the bridge group.
Redundancy Group ID	ID of the redundancy group to which the bridge group belongs.
Admin Failover Priority	Failover priority of the bridge group.
Oper Failover Priority	Active failover priority of the bridge group.
Ethernet Port pull-down menu	Displays the trunk or ports that the bridge group uses to connect to the Ethernet switch.
Vlan	Virtual LAN (VLAN) identifier of the group.
IB Port pull-down menu	Displays the IB port that the bridge group uses.
IB P_KEY	Partition key of the bridge group.
Broadcast Forwarding	Displays a checked box when broadcast forwarding runs.
Broadcast Forwarding Mode	Active broadcast forwarding mode.
Loop Protection Method	Displays the loop protection method of the group.
IP Multicast	Displays a checked box when IP multicasting runs.

Table 6-2 Ethernet Chassis Manager Window Field Descriptions (continued)

Field	Description
Ip Multicast Mode	Active IP multicast mode.
Ip Address	IP address of the bridge group.
Gratuitous IGMP	Displays a checked box when gratuitous IGMP is enabled,
Gratuitous IGMP Mode	The mode in which the gratuitous IGMP was established.
IGMP Version	Selected radio button shows the active IGMP version.
IGMP Version Mode	Active IGMP version mode.
Directed Broadcast	Indicates whether directed broadcasting is enabled for the bridge group.
Directed Broadcast Mode	Active directed-broadcast mode.

Adding Bridge Groups

To create a new bridge group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Groups** branch.

The Bridge Groups table appears in the View frame.

Step 3 Click **Add**.

The Add Ethernet Bridge Group window appears.

Step 4 Enter a bridge group ID number in the ID field.

Step 5 (Optional) Enter a name for the bridge group in the Name field.

Step 6 (Optional) Check the **Enable** check box in the Broadcast Forwarding field to enable broadcast forwarding for this bridge group.

Step 7 Click the **none** radio button or the **one** radio button in the Loop Protection Method field to choose a protection method.

Step 8 (Optional) Check the **Enable** check box in the IP Multicast field to enable IP multicast forwarding.

Step 9 (Optional) Enter and IP address for the bridge group in the IP Address field.

Step 10 (Optional) Check the **Enable** check box in the Gratuitous IGMP field to enable gratuitous IGMP.

Enable this feature when IGMP snooping is enabled on the Ethernet switches connected to the Ethernet gateway.

Step 11 (Optional) In the IGMP Version field, click the **v1**, **v2**, or **v3** radio button to select the IGMP version.

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 12 (Optional) In the Directed Broadcast field, check the **Enable** 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 13 Select a port from the Ethernet Port pull-down menu.

Step 14 Enter a virtual LAN in the Vlan field.

Step 15 Select an IB gateway port from the IB Port pull-down menu.

Step 16 (Optional) Enter a partition key in the IB P_KEY field.

Step 17 Click **Apply**.

Configuring Bridge Groups

To configure the properties of a bridge group, follow these steps:

Step 1 Expand the **Ethernet** icon in the Tree frame.

Step 2 Select the **Bridge Groups** branch.

The Bridge Groups table appears in the View frame.

Step 3 Click the radio button next to the bridge group whose properties you want to view, and then click **Properties**.

The Ethernet Chassis Manager window opens.

Step 4 (Optional) Enter a name for the bridge group in the Name field.

Step 5 (Optional) Select a port from the Ethernet Port pull-down menu.

Step 6 (Optional) Enter a virtual LAN ID in the Vlan field.

Step 7 (Optional) Select a gateway port from the IB Port pull-down menu.

Step 8 (Optional) Enter a partition key in the IB P_KEY field.

Step 9 (Optional) Check (or uncheck) the **Enable** check box in the Broadcast Forwarding field to enable (or disable) broadcast forwarding for the bridge group.

Step 10 (Optional) Click the **none** radio button or **one** radio button in the Loop Protection Method field.

Currently, only one method of loop protection is supported.

Step 11 (Optional) Check (or uncheck) the **Enable** check box in the IP Multicast field to enable (or disable) multicast forwarding for the bridge group.

Step 12 (Optional) Enter an IP address for the bridge group in the IP Address field.

Step 13 (Optional) Check the **Enable** check box in the Gratuitous IGMP field to enable gratuitous IGMP.

Enable this feature when IGMP snooping is enabled on the Ethernet switches connected to the Ethernet gateway.

Step 14 (Optional) In the IGMP Version field, click the **v1**, **v2**, or **v3** radio button to select the IGMP version.

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 15 (Optional) In the Directed Broadcast field, check (or uncheck) the **Enable** check box to enable (or disable) 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 16 Click **Apply**.

Deleting Bridge Groups

To delete a bridge group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame, and then select the **Bridge Groups** branch.

The Bridge Groups table appears in the View frame.

Step 2 Click the radio button next to the bridge group that you want to delete, and click **Delete**.

Note You will not be asked for confirmation after you click Delete. The bridge group is removed immediately.

Viewing and Managing Bridge Subnets

These topics describe how to view and manage bridge subnets:

- Viewing Bridge Subnets, page 6-5
- Adding a Bridge Subnet, page 6-6
- Deleting a Bridge Subnet, page 6-6

Viewing Bridge Subnets

To view bridge subnets, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Subnet** branch.

The Bridge Subnet display appears in the View frame. Table 6-3 describes the fields in this display.

Table 6-3 Bridge Subnets Field Descriptions

Field	Descriptions
ID	Subnet ID number
Subnet Prefix	Subnet prefix, in A.B.C.D format.
Subnet Prefix Len	Length of the subnet prefix.

Adding a Bridge Subnet

To add a bridge subnet, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Subnet** branch.

Step 3 Click **Add**.

The Add Ethernet Bridge Group Subnet window opens.

Step 4 Enter an integer value in the ID field to assign an ID number to the subnet.

Step 5 Enter the subnet prefix in the Subnet Prefix field in A.B.C.D format.

Step 6 Enter an integer value in the Subnet Prefix Len field to configure a length for the subnet prefix.

Step 7 Click **Apply**.

Deleting a Bridge Subnet

To delete a bridge subnet, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Subnet** branch.

Step 3 Click the radio button next to the subnet that you want to delete, and then click **Delete**.

Note You will not be asked for confirmation after you click Delete. The bridge subnet is removed immediately.

Viewing and Managing Bridge Forwarding

These topics describe how to view and manage bridge forwarding:

- Viewing Bridge Forwarding, page 6-6
- Adding Bridge Forwarding, page 6-7
- Deleting Bridge Forwarding, page 6-7

Viewing Bridge Forwarding

To view bridge forwarding, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Forwarding** branch.

The Bridge Forwarding display appears in the View frame. Table 6-4 describes the fields in this display.

Table 6-4 Bridge Forwarding Field Descriptions

Field	Description
ID	Integer-value identifier of the bridge group.
Port Type	Displays eth for IP and ib for IPoIB.
Dest Address	Final destination of the packets.
Dest Length	Number of hops to the destination.
Next Hop	First hop out of the server switch to forward packets that you ultimately want to arrive at the destination.
Subnet Prefix	Subnet prefix of the bridge group.
Prefix Length	Subnet prefix length, in bits, of the bridge group.

Adding Bridge Forwarding

To add bridge forwarding information, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Forwarding** branch.

Step 3 Click **Add**.

The Add Ethernet Bridge Group Forwarding window opens.

Step 4 Enter the ID of the bridge group in the ID field.

Step 5 Click the **eth** or **ib** radio button to specify IP or IPoIB.

Step 6 Enter an IP address in the Destination Address field.

Step 7 Enter the destination length in the Dest Length field.

Step 8 Enter the IP address of the next hop in the Next Hop field.

Step 9 Enter the subnet prefix in the Subnet Prefix field.

Step 10 Enter the subnet prefix length, in bits, in the Prefix Length field.

Step 11 Click **Apply**.

Deleting Bridge Forwarding

To delete a bridge subnet, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Bridge Forwarding** branch.

Step 3 Click the radio button next to the forwarding group that you want to delete, and then click **Delete**.

Note You will not be asked for confirmation after you click Delete. The bridge forwarding group is removed immediately.

Viewing and Managing Redundancy Groups

These topics describe how to view and manage redundancy groups:

- Viewing Redundancy Groups, page 6-8
- Creating a Redundancy Group, page 6-9
- Deleting a Redundancy Group, page 6-10
- Viewing or Editing Redundancy Group Properties, page 6-10

Viewing Redundancy Groups

To view the redundancy groups on your server switch, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Click the **Redundancy Group** branch.

The Redundancy Group display appears in the View menu. Table 6-5 describes the fields in this display.

Table 6-5 Redundancy Group Field Descriptions

Field	Description
ID	ID number of the redundancy group.
Name	Name of the redundancy group.
Multicast PKey	Partition key of the multicast group to which the redundancy group belongs.
Load balancing	Displays enabled if load balancing runs; otherwise displays disabled.
Members	Number of members in the redundancy group.
Gratuitous IGMP	Indicates whether IGMP is enabled.

Creating a Redundancy Group

To create a redundancy group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Redundancy Group** branch.

Step 3 Click **Add**.

An Add Ethernet Redundancy Group window opens.

Step 4 Enter an integer in the ID field.

Step 5 Enter an ASCII text name in the Name field.

Step 6 (Optional) Check the **Enable** check box in the Load Balancing field.

Step 7 (Optional) Check the **Enable** check box in the Broadcast Forwarding Mode field to enable broadcast forwarding for the 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 8 (Optional) Check the **Enable** check box in the Ip Multicast Mode field 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 9 (Optional) Check the **Enable** check box in the Gratuitous IGMP field to enable gratuitous IGMP for this redundancy group.

Gratuitous IGMP applied 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) In the IGMP Version field, click the **v1**, **v2**, or **v3** radio button to select the IGMP version.

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) Check the **Enable** check box in the Directed Broadcast field to enable directed-broadcast mode.

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 **Apply**.

Deleting a Redundancy Group

To delete a redundancy group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Redundancy Group** branch.

Step 3 Click the radio button next to the redundancy group you want to delete, and then click **Delete**.

Note You will not be asked for confirmation after you click Delete. The redundancy group is removed immediately.

Viewing or Editing Redundancy Group Properties

To view redundancy group properties, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Redundancy Group** branch.

Step 3 Click the radio button next to the redundancy group whose properties you want to view.

Step 4 Click **Properties**.

A Redundancy Group Properties window opens. Table 6-6 describes the fields in this window.

Table 6-6 Redundancy Group Properties Field Descriptions

Field	Description
ID	ID number of the redundancy group.
Name	View or edit the name of the redundancy group.
Multicast PKey	View or edit the partition key of the multicast group to which the redundancy group belongs.
Load Balancing	View the status of load balancing in the redundancy group, or alter the status by checking or unchecking the **Enable** check box.
Members	Number of members in the redundancy group.
Action	Provides a pull-down menu of actions to execute with the group. Choose **Fail Over** to cause a failover within the group.
Result	Result of the action that you apply in the Action field.
Broadcast Forwarding Mode	View whether broadcast forwarding mode is enabled for the redundancy group or alter the status by checking or unchecking the **Enable** check box.
IP Multicast Mode	View whether multicast forwarding mode is enabled for the redundancy group or alter the status by checking or unchecking the **Enable** check box.

Table 6-6 Redundancy Group Properties Field Descriptions (continued)

Field	Description
Gratuitous IGMP	View whether gratuitous IGMP is enabled for the redundancy group or alter the status by checking or unchecking the **Enable** check box.
IGMP Version	View the configured version of IGMP or alter the configuration by clicking the corresponding radio button.
Directed Broadcast	View whether directed-broadcast mode is enabled for the redundancy group or alter the status by checking or unchecking the **Enable** check box.

Step 5 Click **Apply** to activate any configuration changes.

Viewing and Managing Trunk Groups

These topics describe how to view and manage trunk groups:

- Viewing Trunk Groups, page 6-11
- Adding a Trunk Group, page 6-13
- Configuring a Trunk Group, page 6-13
- Deleting a Trunk Group, page 6-14

Viewing Trunk Groups

To view the trunk groups on your server switch, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Trunk Groups** branch.

The Trunk Groups table appears in the View frame. Table 6-7 lists and describes the fields in this table.

Table 6-7 Trunk Groups Table Field Descriptions

Field	Description
ID	ID number of the trunk group.
Name	Name of the trunk group.
Port Members	Ports that belong to the trunk group.
Distribution Type	Distribution type of the trunk group. This field displays one of the following types: • **srcMac** bases load distribution on the source MAC address of the incoming packet. Packets from different hosts use different ports in the channel, but packets from the same host use the same port in the trunk group. • **dstMac** bases the load distribution on the destination host MAC address of the incoming packet. Packets to the same destination travel on the same port, but packets to different destinations travel on different ports in the trunk group. • **srcDstMac** bases load distribution on the MAC address of the source logic gate (XOR) destination. • **srcIp** bases the load distribution on the source IP address. Packets from the same source travel on the same port, but packets from different sources travel on different ports in the trunk group. • **dstIp** bases the load distribution on the destination IP address of the incoming packet. Packets to the same destination travel on the same port, but packets to different destinations travel on different ports in the trunk group. • **srcDstIp** bases load distribution on the IP address of the source logic gate (XOR) destination.
Trunk Group Enabled	Displays a checked **Enable** check box to indicate an active trunk group.
MTU	Maximum transmission unit (MTU) of the group.
MAC Address	Media Access Control (MAC) address of the trunk group, such as 00:05:ad:01:59:30. This is a unique physical address associated with the trunk (link-aggregated) interface. This address is separate from the individual port MAC addresses.
IfIndex	Displays a management software unique identifier for all physical and logical (trunks, gateway-ports) interfaces.

Adding a Trunk Group

To add a trunk group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Trunk Groups** branch.

The Trunk Groups table appears in the View frame.

Step 3 Click **Add**.

The Add Ethernet Trunk Group window opens.

Step 4 Enter a trunk group ID number in the ID field.

Step 5 Enter a name for the trunk group in the Name field.

Step 6 In the Port Members field, check the check boxes of the ports that you want to include.

Step 7 Check the check box of a particular card to automatically check all ports on that card.

Step 8 Click the radio button of the distribution type to apply to the trunk group in the Distribution Type field.

Step 9 (Optional) Check the **Trunk Group Enabled** check box to immediately enable the trunk group.

Step 10 Click **Apply**.

Configuring a Trunk Group

To configure an existing trunk group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Trunk Groups** branch.

The Trunk Groups table appears in the View frame.

Step 3 Click the radio button next to the group that you want to delete, and then click **Properties**.

The Ethernet Trunk Group Properties window opens.

Step 4 (Optional) Create or change the name of the trunk group in the Name field.

Step 5 (Optional) Check or uncheck check boxes in the Port Members field to add or remove ports from the group.

Step 6 (Optional) Click a radio button in the Distribution Type field to change the type.

Step 7 (Optional) Check or uncheck the **Enabled** check box in the Trunk Group Enabled field to enable or disable the trunk group.

Step 8 Click **Apply**.

Deleting a Trunk Group

To delete a trunk group, follow these steps:

Step 1 Expand **Ethernet** in the Tree frame.

Step 2 Select the **Trunk Groups** branch.

The Trunk Groups table appears in the View frame.

Step 3 Click the radio button next to the group that you want to delete, and then click **Delete**.

Note You will not be asked for confirmation after you click Delete. The truck group is removed immediately.

CHAPTER 7

Fibre Channel Tasks

This chapter describes the Chassis Manager Fibre Channel tasks and contains these sections:

- Configuring Global ITL Attributes, page 7-1
- Viewing and Managing SRP Hosts (Initiators), page 7-2
- Viewing and Configuring Fibre Channel Targets, page 7-7
- Viewing and Managing Fibre Channel LUNs, page 7-9
- Viewing ITs and IT Properties, page 7-12
- Viewing ITLs and ITL Properties, page 7-14
- Viewing Global Statistics, page 7-15

Configuring Global ITL Attributes

Configure global initiator, target, LUN (ITL) attributes to select the attributes that apply by default to all new ITLs. For detailed information about these attributes, see the *Fibre Channel Gateway User Guide*.

Note If you change ITL attributes, the changes apply only to ITLs created after the change. Existing ITLs do not change.

To configure global attributes, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Global Policies** branch.

The Global Policies display appears in the View frame.

Step 3 Configure host attributes as follows:

a. (Optional) Check the **Restricted** check box in the Gateway Port Access field to follow these steps:

- Check the check box and deny all new initiators access to ports.
- Uncheck the check box and grant all new initiators access to ports.

b. (Optional) Check the **Restricted** check box in the LUN Access field to follow these steps:

- Check the check box and deny all new initiators access to LUNs.
- Uncheck the check box and grant all new initiators access to LUNs.

Step 4 Configure random access device attributes as follows:

a. (Optional) Enter an integer value between 1 and 256 in the ITL HI Mark field.

b. (Optional) Enter an integer value between 1 and 100 in the ITL Max Retries field.

c. (Optional) Enter an integer value between 1 and 1800 in the ITL Min I/O Timeout field.

d. (Optional) In the ITL Dynamic Loading field, click one of the following:

- The **Path Affinity** radio button to enable dynamic path affinity on all new ITLs.
- The **Gateway Port Load Balancing** radio button to enable load balancing among all gateway ports on all new ITLs.
- The **Gateway Port Failover** radio button to enable FC gateway port failover for all new ITLs.

Step 5 Configure sequential access device attributes as follows:

a. (Optional) Enter an integer value between 1 and 256 in the ITL HI Mark field.

b. (Optional) Enter an integer value between 1 and 100 in the ITL Max Retries field.

c. (Optional) Enter an integer value between 1 and 1800 in the ITL Min I/O Timeout field.

d. (Optional) In the ITL Dynamic Loading field, click one of the following:

- The **Path Affinity** radio button to enable dynamic path affinity on all new ITLs.
- The **Gateway Port Load Balancing** radio button to enable load balancing between Fibre Channel gateway ports on all new ITLs.
- The **Gateway Port Failover** radio button to enable FC gateway port failover for all new ITLs.

Step 6 Click **Apply**.

Viewing and Managing SRP Hosts (Initiators)

These topics describe how to view and manage SRP hosts:

- Viewing SRP Hosts (Initiators), page 7-3
- Viewing SRP Host (Initiator) Properties, page 7-3
- Viewing SRP Host (Initiator) World-Wide Port Names, page 7-4
- Viewing IT Policies of the Host, page 7-4
- Viewing ITL Policies of the Host, page 7-5
- Adding a SRP Host, page 7-5
- Deleting a SRP Host, page 7-6
- Configuring SRP Host (Initiator) Properties, page 7-6

Viewing SRP Hosts (Initiators)

To view the SRP hosts that connect to your device and, with your server switch, behave as Fibre Channel initiators, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table of SRP hosts that connect to the chassis appears in the View frame. Table 7-1 describes the fields in this table.

Table 7-1 SRP Hosts Table Field Descriptions

Field	Description
Description	User-assigned text description of the SRP host.
SRP Initiator ID	Host GUID and GUID extension.
WWNN	World-wide node name (WWNN) of the SRP host.
Ports Registered With	Ports on your server switch that connect to the host.

Viewing SRP Host (Initiator) Properties

To view the properties of a SRP host, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the SRP host whose properties you want to view, and then click **Properties**.

The SRP Host Properties window opens. Table 7-2 describes the fields of this window.

Table 7-2 SRP Host Properties Window Fields

Field	Description
SRP Initiator ID	Host GUID and GUID extension.
Ports Registered With	Ports on your server switch that connect to the host.
WWNN	World-wide node name (WWNN) of the SRP host.
Description	User-assigned text description of the SRP host.
PKeys	Partition keys of the SRP host.
Boot Target	WWPN of the target that contains the image that the SRP host uses to boot.
Boot LUN	LUN ID of the LUN that contains the image that the SRP host uses to boot.
Action	Provides a pull-down menu of actions that you can perform on the host. Select an action, and then click **Apply**.

Table 7-2 SRP Host Properties Window Fields (continued)

Field	Description
Result	Displays the result of the action that you performed with the pull-down menu in the Action field.
Alternate Boot Target WWPN	World-wide port name (WWPN) of the alternate target port that the initiator can access through the virtual port.
Alternate Boot FC LUN	Logical unit number of the alternate target device.

Viewing SRP Host (Initiator) World-Wide Port Names

To view the world-wide port names (WWPNs) of the virtual ports through which FC nodes communicate with SRP hosts, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the SRP host whose WWPNs you want to view.

Step 4 Select **Show WWPNs** from the Show Options pull-down menu.

A SRP Host Wwpns table appears in the View frame. Table 7-3 describes the fields in this table.

Table 7-3 SRP Host Wwpns Table Field Descriptions

Field	Description
GUID	GUID of the SRP host.
Extension	GUID extension of the SRP host.
Slot/Port	Physical FC gateway port (in slot#/port# format) that passes traffic (addressed to the virtual port WWPN) to the SRP host.
WWPN	WWPN of the virtual FC port.
FC Address	FC address of the virtual FC port.

Viewing IT Policies of the Host

To view the details of the initiator-target (IT) pairs to which a host (initiator) belongs, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the SRP host whose ITs you want to view.

Step 4 Select **Show IT Policies** from the **Show Options** pull-down menu.

The Show IT display appears in the View frame but lists only ITs that include the initiator that you selected. For more information, see the "Viewing ITs and IT Properties" section on page 7-12 or see Table 7-8.

Viewing ITL Policies of the Host

To view details of the initiator-target-LUN (ITL) groups to which a host (initiator) belongs, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the SRP host whose ITLs you want to view.

Step 4 Select **Show ITL Policies** from the **Show Options** pull-down menu.

The Show ITL display appears in the View frame, but lists only ITLs that include the initiator that you selected. For more information, seethe "Viewing ITLs and ITL Properties" section on page 7-14 or see Table 7-10.

Adding a SRP Host

To add a SRP host to the configuration file, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

An SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click **Add**.

The Add SRP Host window opens.

Step 4 Enter the GUID of the new initiator in the Host GUID field.

Step 5 (Optional) Enter a description for the new initiator in the Description field.

Step 6 Click **Apply**.

Deleting a SRP Host

To delete an SRP host, follow these steps:

Step 1 Expand the **Fibre Channel** icon in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the host that you want to delete from the configuration file, and then click **Delete**.

Configuring SRP Host (Initiator) Properties

To configure properties of a SRP host, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A SRP Hosts table that includes all SRP hosts that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the SRP host whose properties you want to view, and then click **Properties**.

The SRP Host Properties window opens.

Step 4 (Optional) Enter a text description for the SRP host in the Description field.

Step 5 (Optional) Enter a partition key (or comma-separated keys) in the PKeys field.

Step 6 (Optional) Enter the world-wide port name (WWPN) of a target that holds a boot image in the Boot Target field.

Step 7 (Optional) Enter the LUN ID of a disk that holds a boot image in the Boot LUN field.

Step 8 Click **Apply**, and then click **Close**.

Viewing and Configuring Fibre Channel Targets

These topics describe how to view and configure Fibre Channel targets:

- Viewing Fibre Channel Targets, page 7-7
- Viewing Fibre Channel Target Properties, page 7-7
- Configuring Fibre Channel Target Properties, page 7-8
- Viewing IT Policies of the Target, page 7-9
- Viewing ITL Policies of the Target, page 7-9

Viewing Fibre Channel Targets

To view the Fibre Channel targets in the configuration file of your server switch, follow these steps:

Step 1 Expand the **Fibre Channel** icon in the Tree frame.

Step 2 Select the **Targets** branch.

A Targets table that includes all targets in your configuration file appears in the View frame. Table 7-4 describes the fields in this table.

Table 7-4 Targets Table Field Descriptions

Field	Description
WWPN	World-wide port name (WWPN) of the port on the target through which your server switch accesses the target.
Description	User-assigned target description. **Note** If no user has assigned a description, a default description appears.
Physical Access	Port on your server switch (in slot#card# format) through which your server switch accesses the target.
Connection Type	Displays nlport to indicate a virtual FC port or down to indicate a faulty connection.

Viewing Fibre Channel Target Properties

To view the properties of a Fibre Channel target, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Targets** branch.

A Targets table that includes all targets in your configuration file appears in the View frame.

Step 3 Click the radio button next to the target whose properties you want to view, and then click **Properties**.

The SRP Target Properties window opens. Table 7-5 describes the fields in this window.

Table 7-5 SRP Target Properties Window Field Descriptions

Field	Description
WWPN	World-wide port name (WWPN) of the port on the target through which your server switch accesses the target.
WWNN	World-wide node name (WWNN) of the target.
FC Address	Fibre Channel address of the target.
IOC GUID	InfiniBand I/O controller (IOC) through which initiators access the target. On the Cisco SFS 3012 and Cisco SFS 3001 platforms, the IOC identifies a Fibre Channel gateway slot.
Physical Access	Port on your server switch (in slot#/card# format) through which your server switch accesses the target.
MTU	Maximum transmission unit, in bytes, of the target.
Connection Type	The **down** and **nlPort** radio buttons assign a connection type to the target.
Description	User-assigned target description. **Note** If no user has assigned a description, a default description appears.
Service Name	Name of the service to associate with the WWPN.

Configuring Fibre Channel Target Properties

To configure the properties of a Fibre Channel target, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Targets** branch.

A Targets table that includes all targets in your configuration file appears in the View frame.

Step 3 Click the radio button next to the target whose properties you want to view, and then click **Properties**.

The SRP Target Properties window opens.

Step 4 (Optional) Click either the **down** radio button or **nlPort** radio button to configure the connection type of the target.

Step 5 (Optional) Enter a description in the Description field.

Step 6 (Optional) Enter a server name in the Service Name field.

Step 7 Click **Apply**, and then click **Close**.

Viewing IT Policies of the Target

To view the details of the initiator-target (IT) pairs to which a target belongs, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Targets** branch.

A Targets table that includes all FC targets that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the target whose ITs you want to view.

Step 4 Select **Show IT Policies** from the Show Options pull-down menu.

The ITs display appears in the View frame, but lists only ITs that include the target that you selected. For more information, see the "Viewing ITs and IT Properties" section on page 7-12 or see Table 7-8.

Viewing ITL Policies of the Target

To view the details of the initiator-target-LUN (ITL) groups to which a target belongs, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **SRP Hosts** branch.

A Targets table that includes all FC targets that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the target whose ITLs you want to view.

Step 4 Select **Show ITL Policies** from the **Show Options** pull-down menu.

The ITLs display appears in the View frame but lists only ITLs that include the target that you selected. For more information, see the "Viewing ITLs and ITL Properties" section on page 7-14 or see Table 7-10.

Viewing and Managing Fibre Channel LUNs

These topics describe how to view and manager Fibre Channel LUNs:

- Viewing Fibre Channel LUNs, page 7-10
- Viewing Fibre Channel LUN Properties, page 7-10
- Configuring Fibre Channel LUN Properties, page 7-11
- Viewing ITL Policies of the LUN, page 7-12

Viewing Fibre Channel LUNs

To view the logical units (FC storage disks) in the configuration file of your server switch, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Logical Units** branch.

A Logical Units table that includes all LUs in your configuration file appears in the View frame. Table 7-6 describes the fields in this table.

Table 7-6 Logical Units Table Field Descriptions

Field	Description
Logical ID	Logical ID of the logical unit (disk).
Description	User-assigned logical unit description. If no user has assigned a description, a default description appears.
Physical Access	Physical FC gateway ports through which your server switch accesses the LU.

Viewing Fibre Channel LUN Properties

To view Fibre Channel LUN properties, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Logical Units** branch.

A Logical Units table that includes all LUs in your configuration file appears in the View frame.

Step 3 Click the radio button next to the LUN whose properties you want to view, and then click **Properties**.

The SRP LUN Properties window opens. Table 7-7 describes the fields in this window.

Table 7-7 SRP LUN Properties Window Field Descriptions

Field	Description
Logical ID	Logical ID of the LUN.
Device Category	Provides the **random** radio button and **sequential** radio button to identify disk devices and tape devices respectively.
Inquiry Data	SCSI inquiry data retrieved about the LU.
Physical Access	Ports on your server switch that can access the LUN.
Description	User-assigned description of the LUN.
Hi Mark	The maximum number of outstanding requests from the initiator to the storage that the ITL can maintain.
Max Retry	Number of failed communication attempts that must occur before the LUN identifies the initiator as inaccessible.

Table 7-7 SRP LUN Properties Window Field Descriptions (continued)

Field	Description
Min IO Timeout	Maximum amount of time that elapses before a SRP request times out.
Size	Size of the LUN.
Dynamic Pathing	Provides the following radio buttons: Path Affinity This feature locks a storage connection to a path for the duration of data transfer to increase speed and efficiency. Gateway Port Load Balancing This feature distributes traffic evenly across both ports in an FC gateway card (when both of the ports can access the same storage). Gateway Port Failover This feature leaves one port on an FC gateway dormant so it can adopt the traffic of the other port (when both of the ports can access the same storage) if that port goes down.

Configuring Fibre Channel LUN Properties

To configure Fibre Channel LUN properties, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Logical Units** branch.

A Logical Units table that includes all LUs in your configuration file appears in the View frame.

Step 3 Click the radio button next to the LUN whose properties you want to view, and then click **Properties**.

The SRP LUN Properties window opens.

Step 4 (Optional) Enter a description in the Description field.

Step 5 (Optional) Enter an integer value in the Hi Mark field.

Step 6 (Optional) Enter an integer value in the Max Retry field.

Step 7 (Optional) Enter an integer value in the Min IO Timeout field.

Step 8 (Optional) Click a radio button in the Dynamic Pathing field.

Step 9 Click **Apply**, and then click **Close**.

Viewing ITL Policies of the LUN

To view the details of the initiator-target-LUN (ITL) groups to which a LUN belongs, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Logical Units** branch.

A Logical Units table that includes all FC targets that connect to the chassis appears in the View frame.

Step 3 Click the radio button next to the LUN whose ITLs you want to view.

Step 4 Select **Show ITL Policies** from the Show Options pull-down menu.

The **ITLs** display appears in the View frame but lists only ITLs that include the LUN that you selected. For more information, see the "Viewing ITLs and ITL Properties" section on page 7-14 or see Table 7-10.

Viewing ITs and IT Properties

These topics describe how to view ITs and their properties:

- Viewing ITs, page 7-12
- Viewing IT Properties, page 7-13

Viewing ITs

To view Initiator-Target (IT) pairs on your server switch, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **ITs** branch.

The ITs table appears in the View frame. Table 7-8 describes the fields in this table.

Table 7-8 ITs Table Field Descriptions

Field	Description
SRP Initiator ID	GUID of the initiator (host).
Target WWPN	WWPN of the target.
Current Access	Physical FC gateway port through which the host currently accesses the target.
Physical Access	Physical FC gateway ports through which the host can access the target.

Viewing IT Properties

To view detailed Initiator-Target (IT) pair properties, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **ITs** branch.

The ITs table appears in the View frame.

Step 3 Click the radio button next to the IT pair whose properties you want to view, and then click **Properties**.

The SRP IT Properties window opens. Table 7-9 describes the fields in this window.

Table 7-9 SRP IT Properties Window Field Descriptions

Field	Description
SRP Initiator ID	GUID of the host.
Target WWPN	WWPN of the target.
Description	User-assigned description of the IT.
Current Access	Physical FC gateway port through which the host currently accesses the target.
Physical Access	Physical FC gateway ports through which the host can access the target.
Port Mask	Displays a check box for every FC gateway card and FC gateway port on the chassis. Ports with a checked check box grant the initiator access to the target.
Mode	The active radio button in this field represents the mode configuration. The Normal radio button configures the IT pair to behave normally and the Test radio button configures the gateway to do ITL logins for this IT without the participation of the HBA of the initiator. You cannot change the mode of an IT pair to test.
Action pull-down menu	Discovers ITLs that the initiator can form with the LUNs in the target.
Result	Displays the status of the action if you select **Discover ITLs** from the Action pull-down menu and then click **Apply**.

Viewing ITLs and ITL Properties

These topics describe how to view ITLs and their properties:

- Viewing ITLs, page 7-14
- Viewing ITL Properties, page 7-14

Viewing ITLs

To view Initiator-Target-LUN (ITL) properties, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **ITLs** branch.

The ITLs table appears in the View frame. Table 7-10 describes the fields in this table.

Table 7-10 ITLs Table Field Descriptions

Field	Description
SRP Initiator ID	GUID of the initiator (host).
Target WWPN	WWPN of the target.
FC LUN ID	Fibre Channel ID of the disk or tape in the target. The ID of the first LUN is always 00:00:00:00:00:00:00:00, and the IDs for subsequent LUNs increment by 1 in hexadecimal.
LUN Logical ID	Logical ID of the disk or tape in the target.

Viewing ITL Properties

To view detailed Initiator-Target-LUN (ITL) properties, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **ITLs** branch.

The ITLs table appears in the View frame.

Step 3 Click the radio button next to the ITL whose properties you want to view, and then click **Properties**.

The SRP ITL Properties window opens. Table 7-11 describes the fields in this window.

Table 7-11 SRP ITL Properties Window Field Descriptions

Field	Description
SRP Initiator ID	GUID of the initiator (host).
Target WWPN	WWPN of the target.

Table 7-11 SRP ITL Properties Window Field Descriptions (continued)

Field	Description
FC LUN ID	Fibre Channel ID of the disk or tape in the target. The ID of the first LUN is always **00:00:00:00:00:00:00:00**, and the IDs for subsequent LUNs increment by 1 in hexadecimal notation.
LUN Logical ID	Logical ID of the disk or tape in the target.
Device Category	Identifies a LUN as random (a disk) or sequential (a tape).
Description	User-assigned text identifier of the ITL.
SRP LUN ID	SRP ID of the disk or tape in the target. The ID of the first LUN is always 00:00:00:00:00:00:00:00, and the IDs for subsequent LUNs increment by 1 in hexadecimal notation.
Physical Access	Physical FC gateway port through which the host currently accesses the LUN.
Current Access	Physical FC gateway ports through which the host can access the LUN.
Port Mask	Displays a check box for every FC gateway card and FC gateway port on the chassis. Ports with a checked check box grant the initiator access to the LUN.

Viewing Global Statistics

To view global SRP statistics, follow these steps:

Step 1 Expand **Fibre Channel** in the Tree frame.

Step 2 Select the **Global Statistics** branch.

The SRP Global Statistics display appears in the View frame. Table 7-12 describes the fields in this display.

Table 7-12 SRP Global Statistics Display Field Descriptions

Field	Description
Link Events	Total number of link events (link up, link down) processed by the Fibre Channel interface gateways.
SRP Initiated IOs	Total number of I/O transactions requested by the SRP initiator.
SRP Commands Completed	Total number of SRP commands completed on the Fibre Channel interface gateways.
SRP Bytes Read	Total number of I/O bytes read by the SRP initiator that is connected to this chassis.
SRP Bytes Written	Total number of I/O bytes written by the SRP initiator.
SRP Connections	Total number of connections used by the SRP initiator.
SRP Commands Outstanding	Total number of SRP commands outstanding on the Fibre Channel interface gateways.

Table 7-12 SRP Global Statistics Display Field Descriptions (continued)

Field	Description
SRP Errors	Total number of SRP errors encountered on the Fibre Channel interface gateways.
FCP Initiated IOs	Total number of I/O responses by the Fibre Channel device to SRP initiator requests.
FCP Commands Completed	Total number of FCP commands completed on the Fibre Channel interface gateways.
FCP Bytes Read	Total number of I/O bytes read by the target device.
FCP Bytes Written	Total number of I/O bytes written by the target device.
FCP Commands Outstanding	Total number of FCP commands outstanding on the Fibre Channel interface gateways.
FCP Errors	Total number of FCP errors encountered on the Fibre Channel interface gateways.

INDEX

A

access privileges 2-9
admin status, configuring cards 3-7
audience ix
authentication, assigning a method 4-13
authentication failures 1-4, 4-21
autonegotiation
  configuring 3-14
  description of 3-20
autonegotiation, configuring 3-14

B

backing up configuration files 4-10
backplane, viewing 3-19
baud rate 3-19
boot configuration, setting 4-9
bridge forwarding
  adding 6-7
  deleting 6-7
  viewing 6-6
bridge groups
  adding 6-3
  configuring 6-4
  deleting 6-5
  properties 6-2
  viewing 6-1
bridge subnets
  adding 6-6
  deleting 6-6
  viewing 6-5
bridging, port 3-11
broadcast forwarding
  bridge group 6-4
  redundancy group 6-9
browser requirements 1-7

C

cards
  admin status, configuring 3-7
  inventory 3-6
  test results 4-22
  viewing 3-1
  viewing properties 3-3
Chassis Manager
  launching 2-4
  starting 2-4
chassis manager
  logging out of 2-8
CLI authentication 4-13
configuration files
  backing up 4-10
  boot config, setting 4-9
  exporting 4-9
  importing 4-8
  saving 4-11
conventions x
current status
  card 3-4
  ports 3-20

D

data bits 3-19

date, configuring 4-4
daylight savings time, configuring 4-5
DHCP server 2-3
directed broadcasting
  bridge group 6-4
  redundancy group 6-9
DNS system service
  assigning 4-12
  description of 1-4
documentation
  conventions x
  organization ix

E

encryption key, configuring
  RADIUS server 4-16
  TACACS server 4-19
Ethernet management port
  configuring IP address 2-2
  viewing attributes of 3-20
exporting
  configuration files 4-9
  log files 4-9

F

fan
  status 3-17
  test results 4-23
files, deleting 4-7
file system
  deleting files 4-7
  viewing 4-6
filter indicator 2-8
frames, GUI
  system 1-1
  Tree 1-2
  View 1-6
FRU errors
  card 4-24
  fan 4-24
  power supply 4-25
  viewing 1-4
FRU number, card 3-5
FRU test results
  card 4-24
  fan 4-24
  power supply 4-25
FTP system service 1-4
  disabling 4-12
  enabling 4-12

G

gateway ports, internal 3-7
global ITL
  attributes 7-1
  policies 7-1
  statistics 7-15
gratuitous IGMP
  bridge group 6-4
  redundancy group 6-9

H

Hop Count 5-3
HoQ life 5-3
hosts
  adding 7-5
  configuring 7-6
  deleting 7-6
  ITLs 7-5
  ITs 7-4
  properties 7-3
  viewing 7-2

WWPNs 7-4
host-target-LUN policies 7-14
host-target-LUN properties 7-14
host-target policies 7-12
host-target properties 7-13
HTTP
authentication failures 1-4, 4-21
configuring 4-15
enabling 2-4
viewing 1-4
HTTPS
configuring 4-15
enabling 2-4

I

IB counter reset 4-3
IGMP version
bridge group 6-4
redundancy group 6-9
image files, importing 4-8
InfiniBand counters
clearing per port 3-15
resetting global 4-4
InfiniBand management port, viewing attributes of 3-20
InfiniBand nodes
neighbors 5-10
properties 5-8
viewing 5-7
InfiniBand ports
properties 5-11
viewing 5-10
initiators
adding 7-5
configuring 7-6
deleting 7-6
ITLs 7-5
ITs 7-4
properties 7-3
viewing 7-2
WWPNs 7-4
installing software 4-8
internal gateway ports 3-7
IOCs
properties 5-19
services 5-21
viewing 5-19
IOUs 5-18
IP address, Ethernet management port
configuring 2-2
viewing 3-20
IT
policies 7-12
properties 7-13
ITL
global attributes 7-1
global policies 7-1
policies 7-14
properties 7-14

L

location 4-3
locator 2-8
log files, exporting 4-9
loop protection method 6-4
LUNs
configuring 7-11
ITLs 7-12
properties 7-10
viewing 7-9

M

MAC (media access control) 3-20
MAC Address 3-9
MadRetries 5-5

management ports, viewing 3-19
Max Retries 4-20
max retry
  configuring for RADIUS 4-17
  configuring for TACACS 4-20
media access control (MAC) address 3-20
MTU 3-9
multicast forwarding
  bridge group 6-4
  redundancy group 6-9

N

name
  configuring port names 3-13
  file 4-7
  switch name 4-2
neighbor properties, viewing 5-17
neighbors, InfiniBand 5-16
net mask, ports 3-20
node neighbors, viewing 5-10
node ports, viewing 5-10
nodes
  properties 5-8
  viewing 5-7
  viewing neighbors 5-10
  viewing ports 5-10
NodeTimeout 5-5
NTP servers, assigning 4-5

O

operational state, card 3-4
organization ix

P

parity 3-19
PCA
  assembly number for card 3-5
  serial number for card 3-5
platform requirements 1-8
port bridging properties 3-11
ports
  administrative status 3-20
  autonegotiation 3-14
  bridging properties 3-11
  current status 3-20
  disabling 3-13
  enabling 3-13
  gateway 3-20
  InfiniBand, viewing 5-10
  InfiniBand counters, clearing 3-15
  IP address 3-20
  management ports 3-19
  name, configuring 3-13
  net mask 3-20
  node ports 5-10
  properties, configuring 3-13
  properties, viewing 3-8
  speed, configuring 3-14
  viewing all 3-8
  view internal gateway 3-7
ports, InfiniBand properties 5-11
POST errors
  fan 4-23
  power supply 4-23
  viewing 1-4
POST tests 4-23
power supply
  status 3-15
  test results 4-23
prepare your switch 2-1
prerequisites 2-1
printed circuit assembly (PCA) 3-5

R

RADIUS server
- adding 4-17
- configuring 1-4, 4-16
- configuring encryption key 4-16
- configuring max retry value 4-17
- configuring timeout 4-16
- configuring UDP port 4-16
- deleting 4-18
- viewing 4-15

RADIUS system service 1-4
rebooting 4-11
redundancy groups
- creating 6-9
- deleting 6-10
- properties 6-10
- viewing 6-8

related documentation xi
reloading 4-11

S

SA MAD Queue Depth
- configuring 5-5
- viewing 5-3

serial management port, viewing attributes of 3-19
serial number 3-5
services (basic), configuring 4-11
setup 2-1
slot ID 3-4
software, installing 4-8
speed, port speed 3-14
SRP Hosts
- adding 7-5
- configuring 7-6
- deleting 7-6
- ITLs 7-5
- ITs 7-4
- properties 7-3
- viewing 7-2
- WWPNs 7-4

statistics, global ITL 7-15
status, viewing chassis 2-9
stop bits 3-19
subnet manager
- adding 5-4
- CA link HoQ life 5-3
- deleting 5-4
- LID mask control
  - configuring 5-5
  - viewing 5-3
- MAD retries
  - configuring 5-5
  - viewing 5-3
- master poll interval
  - configuring 5-5
  - viewing 5-3
- master poll retries
  - configuring 5-5
  - viewing 5-3
- max active SMs
  - configuring 5-5
  - viewing 5-3
- maximum hop count 5-3
- node timeout
  - configuring 5-5
  - viewing 5-3
- priority
  - configuring 5-5
  - viewing 5-2
- properties
  - configuring 5-4
  - viewing 5-2
- response timeout
  - configuring 5-5
  - viewing 5-2
- SA MAD queue depth

configuring 5-5
viewing 5-3
sweep interval 5-5
configuring 5-5
viewing 5-2
switch lifetime
configuring 5-5
viewing 5-3
switch link HoQ life
configuring 5-5
viewing 5-3
viewing 5-1
wait report response
enabling 5-5
viewing 5-3
subnet services
properties 5-6
viewing 5-6
switch configuration 2-1
Syslog system service
assigning 4-13
viewing 1-4
System frame 1-1
system information
configuring 4-1
viewing 4-2
system operation mode, configuring 4-3

T

TACACS server
adding 4-20
configuring 1-4, 4-19
configuring encryption key 4-19
configuring max retry value 4-20
configuring timeout 4-19
configuring UDP port 4-19
deleting 4-21
viewing 4-18
TACACS system service 1-4
targets
configuring 7-8
ITLs 7-9
ITs 7-9
properties 7-7
viewing 7-7
technical support, defining 4-3
technical support, defining resource 4-3
Telnet system service
disabling 4-12
enabling 4-12
viewing 1-4
temperature sensor status 3-18
tiered locator 2-8
time, configuring 4-4
timeout
configuring for RADIUS server 4-16
configuring for TACACS server 4-19
time zone, configuring 4-5
Tree frame 1-2
trunk groups
adding 6-13
configuring 6-13
deleting 6-14
properties 6-11
viewing 6-11
type, card 3-4

U

UDP authentication 4-19
UDP port, configuring
RADIUS server 4-16
TACACS server 4-19

V

VFrame 4-3
View frame 1-6

W

WaitReportResponse 5-5