



## **Cisco SFS 7000 Series Product Family Chassis Manager User Guide**

Release 2.7.0

### **Corporate 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: 408 526-4100

Text Part Number: OL-9162-02



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.



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 7000 Series Product Family Chassis Manager User Guide*  
© 2006 Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>ix</b>
Audience	ix
Organization	ix
Conventions	x
Related Documentation	xi
Obtaining Documentation	xi
Cisco.com	xi
Product Documentation DVD	xii
Ordering Documentation	xii
Documentation Feedback	xii
Cisco Product Security Overview	xii
Reporting Security Problems in Cisco Products	xiii
Obtaining Technical Assistance	xiii
Cisco Technical Support & Documentation Website	xiv
Submitting a Service Request	xiv
Definitions of Service Request Severity	xiv
Obtaining Additional Publications and Information	xv

---

## CHAPTER 1

<b>About Chassis Manager</b>	<b>1-1</b>
Introduction	1-1
System Frame	1-1
Tree Frame	1-2
Tree Frame Branches	1-3
View Frame	1-6
Browser Requirements	1-7
Platform Requirements	1-7

---

## CHAPTER 2

<b>Getting Started</b>	<b>2-1</b>
Preparing Your Device	2-1
Launching Chassis Manager	2-2
Launching Chassis Manager without SSL	2-2
Launching Chassis Manager with SSL	2-3
Netscape/Mozilla	2-3

Internet Explorer	2-4
Avoiding Error Messages	2-6
Logging Out of Chassis Manager	2-6
Navigating Chassis Manager	2-6
Moving Backward	2-7
Refreshing Views	2-7
Understanding Access Privileges	2-7
Viewing the Device Status	2-8

## CHAPTER 3

### Chassis Tasks 3-1

Viewing Cards on a Chassis	3-1
Viewing Card Properties	3-4
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 Port Properties	3-8
Viewing Port Bridging Properties	3-11
Viewing Port Statistics	3-11
Configuring Ports	3-12
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
Viewing Power Supply Status	3-15
Viewing Power Supply Properties	3-16
Viewing Fan Status	3-17
Viewing Fan Properties	3-17
Viewing Temperature Sensor Status	3-18
Viewing the Backplane Information	3-18
Viewing Management Ports on a Chassis	3-19

## 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 Technical Support Resource	4-3

Configuring System Global Settings	4-3
Configuring System Operation Mode	4-3
Enabling InfiniBand Counter Reset	4-4
Configuring Date and Time Properties	4-4
Configuring the Date and Time	4-4
Assigning NTP Servers	4-5
Viewing Files in the File System	4-5
Deleting Files in the File System	4-6
Installing Software Images	4-6
Importing Configuration Files and Image Files with FTP or SCP	4-7
Exporting Configuration Files and Log Files with FTP or SCP	4-7
Customizing the Boot Configuration	4-8
Backing Up the Running Configuration File	4-8
Saving a Configuration File	4-9
Rebooting the Device	4-9
Configuring Basic Services	4-9
Assigning a DNS Server	4-10
Enabling or Disabling the FTP Access	4-10
Enabling or Disabling the Telnet Access	4-10
Assigning a Syslog Server	4-11
Assigning an Authentication Method	4-11
Configuring HTTP and HTTPS	4-12
Viewing RADIUS Servers	4-12
Viewing and Configuring RADIUS Server Properties	4-13
Adding RADIUS Servers	4-14
Deleting RADIUS Servers	4-14
Viewing TACACS Servers	4-15
Viewing and Configuring TACACS Server Properties	4-16
Adding TACACS Servers	4-17
Deleting TACACS Servers	4-17
Viewing Authentication Failures	4-18
Viewing Diagnostic Test Results	4-18
Viewing Card POST Test Results	4-19
Viewing Fan POST Test Results	4-19
Viewing Power Supply POST Test Results	4-20
Viewing FRU Errors	4-20

---

**CHAPTER 5****InfiniBand Tasks 5-1**

- Viewing Subnet Managers 5-1
  - Viewing Subnet Manager Properties 5-2
  - Adding a Subnet Manager 5-3
  - Deleting a Subnet Manager 5-4
  - Configuring Subnet Manager Properties 5-4
- Viewing InfiniBand Services 5-5
  - Viewing InfiniBand Service Properties 5-6
- Viewing InfiniBand Nodes 5-7
  - Viewing Node Properties 5-7
  - Viewing Node Ports 5-9
  - Viewing Node Neighbors 5-10
- Viewing InfiniBand Ports 5-10
  - Viewing InfiniBand Port Properties 5-11
- Viewing Neighboring InfiniBand Devices 5-15
  - Viewing InfiniBand Neighbor Properties 5-16
- Viewing IOUs 5-17
- Viewing IOCs 5-17
  - Viewing IOC Properties 5-18
- Viewing IOC Services 5-19
  - Viewing Properties of IOC Services 5-20

---

**CHAPTER 6****Ethernet Tasks 6-1**

- Viewing Bridge Groups 6-1
  - Viewing Bridge Group Properties 6-2
  - Adding Bridge Groups 6-3
  - Configuring Bridge Groups 6-3
  - Deleting Bridge Groups 6-4
- Viewing Bridge Subnets 6-4
  - Adding a Bridge Subnet 6-5
  - Deleting a Bridge Subnet 6-5
- Viewing Bridge Forwarding 6-6
  - Adding Bridge Forwarding 6-6
  - Deleting Bridge Forwarding 6-7
- Viewing Redundancy Groups 6-7
  - Creating a Redundancy Group 6-8
    - Deleting a Redundancy Group 6-8
  - Viewing Redundancy Group Properties 6-9

Viewing Trunk Groups	6-10
Adding a Trunk Group	6-11
Viewing Trunk Group Properties	6-11
Configuring a Trunk Group	6-12
Deleting a Trunk Group	6-13

---

**CHAPTER 7**
**FibreChannel Tasks 7-1**

Configuring Global ITL Attributes	7-1
Viewing SRP Hosts (Initiators)	7-2
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 SRP Host	7-5
Deleting SRP Host	7-5
Configuring SRP Host (Initiator) Properties	7-6
Viewing FibreChannel Targets	7-6
Viewing FibreChannel Target Properties	7-7
Configuring FibreChannel Target Properties	7-8
Viewing IT Policies of the Target	7-8
Viewing ITL Policies of the Target	7-9
Viewing FibreChannel LUNs	7-9
Viewing FibreChannel LUN Properties	7-10
Configuring FibreChannel LUN Properties	7-11
Viewing ITL Policies of the LUN	7-11
Viewing ITs	7-12
Viewing IT Properties	7-12
Viewing ITLs	7-13
Viewing ITL Properties	7-14
Viewing Global Statistics	7-15

---

**INDEX**







## Preface

---

This preface describes who should read the *Cisco SFS 7000 Series 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](#)
- [Obtaining Documentation, page xi](#)
- [Documentation Feedback, page xii](#)
- [Cisco Product Security Overview, page xii](#)
- [Obtaining Technical Assistance, page xiii](#)
- [Obtaining Additional Publications and Information, page xv](#)

## 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	<a href="#">About Chassis Manager</a>	Describes Chassis Manager fundamentals.
Chapter 2	<a href="#">Getting Started</a>	Describes how to get started with Chassis Manager.
Chapter 3	<a href="#">Chassis Tasks</a>	Describes how to view the component status on the chassis and configure ports.
Chapter 4	<a href="#">Maintenance Tasks</a>	Describes the tasks for configuring the basic system operation.

Chapter	Title	Description
Chapter 5	<a href="#">InfiniBand Tasks</a>	Describes the tasks for displaying and configuring the InfiniBand operation.
Chapter 6	<a href="#">Ethernet Tasks</a>	Describes the tasks for displaying and configuring the Ethernet operation.
Chapter 7	<a href="#">FibreChannel Tasks</a>	Describes the tasks for displaying and configuring the Fibre Channel operation.

## Conventions

This document uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> . Bold text indicates Chassis Manager elements or text that you must enter as-is.
<i>italic font</i>	Arguments in commands for which you supply values are in <i>italics</i> . Italics not used in commands indicate emphasis.
<b>Menu1 &gt; Menu2 &gt; Item...</b>	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, { <b>interface</b> <i>interface</i> <b>type</b> }.
[ 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.
<b>boldface screen font</b>	Information you must enter is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	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 publication.

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 7000P series switches and command-line interface (CLI) commands, refer to the following:
  - *Release Notes for Cisco SFS 7000P Series Switch Software Release 2.5.0*
  - *Cisco SFS 7000 Series Product Family Element Manager User Guide*
  - *Cisco SFS 7000 Series Product Family Command Reference Guide*
- For detailed hardware configuration and maintenance procedures, see these hardware guides:
  - *Cisco SFS 7000P Switch Installation and Configuration Note*
  - *Cisco SFS 7008P Switch Installation and Configuration Note*
  - *Cisco SFS 7000P Hardware Installation Guide*
  - *Cisco SFS 7008P Hardware Installation Guide*

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>





# About Chassis Manager

Chassis Manager runs directly on your Server Switch to perform administration tasks. This chapter discusses the various components of the interface. Chassis Manager runs on all Server Switches.

This chapter contains these sections:

- [Introduction, page 1-1](#)
- [Browser Requirements, page 1-7](#)
- [Platform Requirements, page 1-7](#)

## Introduction

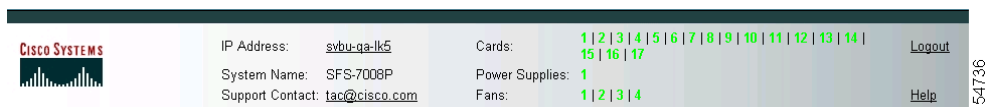
Chassis Manager runs in a standard web browser and displays information in standard HTML formats. The GUI has three frames:

- System Frame, (see [Figure 1-1](#)).
- Tree Frame (see [Figure 1-2](#)).
- View Frame (see [Figure 1-3](#)).

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

**Figure 1-1**      **System Frame**



Click the IP address in the IP Address field of the System frame to open a Telnet window that launches a CLI session to the switch. Click the e-mail address in the Support Contact field to send an e-mail to technical support. Click **Help** to open the online help.

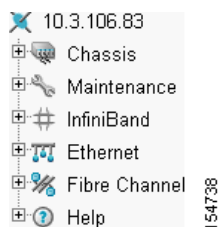
**Table 1-1** *FRU Color Indicators*

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

## 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.

**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 2-7.

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, etc.
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.

**Table 1-2** *Tree Frame Icons (continued)*

Icon	Description
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.

## Tree Frame Branches


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: <ul style="list-style-type: none"> <li>Serial displays the Serial Console port configuration.</li> <li>Ethernet displays the Ethernet Management port configuration.</li> <li>InfiniBand displays the InfiniBand Management port configuration.</li> </ul>

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	<p>Expand the Services icon to display the following branches:</p> <ul style="list-style-type: none"> <li>• General           <p>Displays the following system services and lets you configure them:</p> <ul style="list-style-type: none"> <li>– DNS</li> <li>– FTP</li> <li>– Telnet</li> <li>– Syslog</li> <li>– RADIUS</li> <li>– TACACS+</li> <li>– HTTP</li> </ul> <p>Displays HTTP properties and configuration options.</p> </li> <li>• Radius Servers           <p>Displays the RADIUS server(s) that your device can use to authenticate user logins and lets you configure attributes of the server(s).</p> </li> <li>• Tacacs Servers           <p>Displays the TACACS+ server(s) that your device can use to authenticate user logins and lets you configure attributes of the server(s).</p> </li> <li>• Authentication Failures           <p>Lists CLI, SNMP, and HTTP authentication failures.</p> </li> </ul>
Diagnostics	<p>Expand this branch to view Server Switch diagnostic data in the following branches:</p> <ul style="list-style-type: none"> <li>• POST</li> <li>• Fru Error</li> </ul>

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: <ul style="list-style-type: none"> <li>Nodes Click this branch to view the IB nodes in your IB fabric.</li> <li>Ports Click this branch to view the IB ports in your IB fabric.</li> <li>Neighbors Click this branch to display the interconnecting IB nodes and relevant ports in your IB fabric.</li> </ul>
Device Management (select hardware platforms only)	Expand the Device Management icon to display the following branches: <ul style="list-style-type: none"> <li>IOU Click this branch to view the I/O unit on your Server Switch.</li> <li>IOCs Click this branch to view the controller(s) on your device.</li> <li>IOC Services Click this branch to view the IB features on your device.</li> </ul>

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 InfiniBand 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 table that appears in the View frame when you expand **Chassis** and click the **Ports** branch.

**Figure 1-3 View Frame****Ports**

10.3.102.66 &gt; Chassis &gt; Ports

Properties Refresh Show Options... ▼

	Port	Name	Type	Admin Status	Oper Status	MTU
<input type="radio"/>	5/1	5/1	fc2GFX	up	up	2048
<input type="radio"/>	5/2	5/2	fc2GFX	up	up	2048
<input type="radio"/>	7/1	7/1	fc2GFX	up	down	2048
<input type="radio"/>	7/2	7/2	fc2GFX	up	up	2048
<input type="radio"/>	16/1	16/1	ib4xTX	up	down	4096
<input type="radio"/>	16/2	16/2	ib4xFX	up	up	2048
<input type="radio"/>	16/3	16/3	ib4xTX	up	down	4096
<input type="radio"/>	16/4	16/4	ib4xFX	up	up	2048
<input type="radio"/>	16/5	16/5	ib4xFX	up	up	2048
<input type="radio"/>	16/6	16/6	ib4xTX	up	down	4096
<input type="radio"/>	16/7	16/7	ib4xTX	up	down	4096
<input type="radio"/>	16/8	16/8	ib4xTX	up	down	4096
<input type="radio"/>	16/9	16/9	ib4xFX	up	up	2048
<input type="radio"/>	16/10	16/10	ib4xTX	up	down	4096
<input type="radio"/>	16/11	16/11	ib4xTX	up	down	4096
<input type="radio"/>	16/12	16/12	ib4xTX	up	down	4096

r3g

## 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







# 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 2-2](#)
- [Navigating Chassis Manager, page 2-6](#)
- [Understanding Access Privileges, page 2-7](#)
- [Viewing the Device Status, page 2-8](#)

## Preparing Your Device

To launch Chassis Manager on your Server Switch, you must do 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 2-2](#). Otherwise, to prepare your device, follow these steps:



---

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

---

---

**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)#
```

## ***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- 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** 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 6** 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 7** Enter the **no shutdown** command to enable the Ethernet Management port.

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

- Step 8** Enter the **exit** command to return to global configuration mode.

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

- Step 9** Enable HTTP and/or HTTPS services.

- a. (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
```

- b. (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. This section describes how to do both procedures.

### Launching Chassis Manager without SSL

To launch Chassis Manager without SSL, follow these steps:

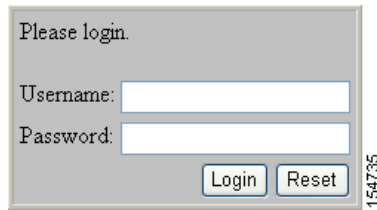
---

- 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 5](#) of “Preparing Your Device” section on page 2-1).

A login window opens. [Figure 2-1](#) displays the login window.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Figure 2-1** Chassis Manager Login Window



- Step 3** Enter your Server Switch username and password in the login window and click **OK** .  
Chassis Manager loads in your browser window.
- 

## Launching Chassis Manager with SSL

SSL setups vary by browser types. The following sections explain how to launch Chassis Manager with SSL using particular browsers.

### 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 5](#) 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 **OK** .  
Chassis Manager loads in your browser window.
-

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## 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 5](#) of “Preparing Your Device” section on page 2-1.)
- Step 3** Press **Enter**.  
A Security Alert window opens.

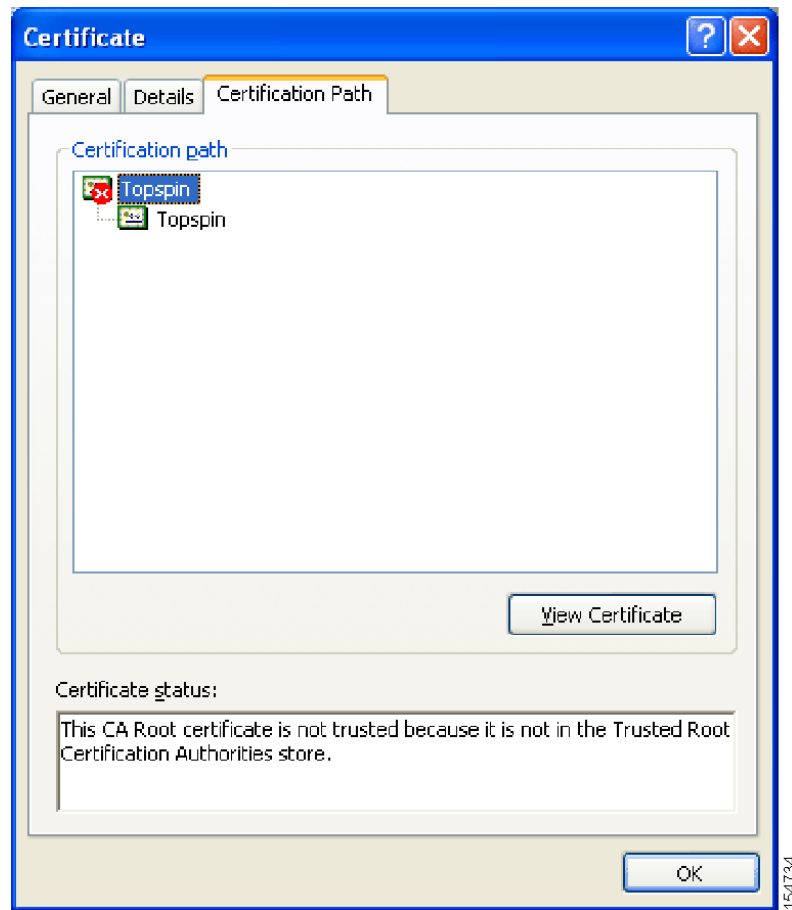
**Figure 2-2 Security Alert Window**



- 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 screen in [Figure 2-3](#).

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Figure 2-3** Certification Path



- 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**.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## 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: **xxxxxx**
  - Step 2** Enter the **enable** command to enter Privileged EXEC mode.  
 SFS-270> **enable**  
 SFS-270#
  - Step 3** Enter the **configure terminal** command to enter global configuration mode.  
 SFS-270# **configure terminal**  
 SFS-270(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-270(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

## *Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

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.

## 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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## 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.





## Chassis Tasks

---

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

- [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 3-12](#)
- [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 3-18](#)
- [Viewing Management Ports on a Chassis, page 3-19](#)

## Viewing Cards on a Chassis

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.

**Table 3-1**      **Cards Table Field Descriptions (continued)**

Field	Description
Operational State	<p>Displays the general condition of the interface card. The general condition may appear as any of the following:</p> <ul style="list-style-type: none"> <li>• unknown</li> <li>• normal</li> <li>• bootFailed</li> <li>• tooHot</li> <li>• booting</li> <li>• checkingBootImage</li> <li>• wrongBootImage</li> <li>• rebooting</li> <li>• standby</li> <li>• recoveryImage</li> </ul> <p>A condition of unknown indicates an unsupported interface card. To address this condition, replace the card with a supported card.</p> <p>The operational state of a card must appear as normal for the current status of the card to appear as up.</p> <p>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.</p> <p>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.</p> <p>When your card overheats, the tooHot condition appears in the show card command output. Expand <b>Chassis</b> and select the <b>Fans</b> branch to see if your fans have failed.</p> <p>The booting condition indicates that the card has not finished loading the necessary image data for the internal configuration.</p>

**Table 3-1**      **Cards Table Field Descriptions (continued)**

Field	Description
Boot Stage	Boot Stage appears as one of the following: <ul style="list-style-type: none"><li>• recovery</li><li>• ipl</li><li>• ppcboot</li><li>• fpga</li><li>• pic</li><li>• ib</li><li>• rootfs</li><li>• kernel</li><li>• exe</li><li>• done</li></ul>
Boot Status	Boot Status may appear as any of the following: <ul style="list-style-type: none"><li>• upgrading</li><li>• success</li><li>• failed</li><li>• badVersion</li><li>• badCrc</li><li>• memoryError</li><li>• outOfSpace</li><li>• programmingError</li><li>• hardwareError</li><li>• fileNotFound</li><li>• inProgress</li></ul>

**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 <b>Apply</b> 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	<p>Displays the general condition of the interface card. The general condition may be any of the following:</p> <ul style="list-style-type: none"> <li>unknown</li> <li>normal</li> <li>wrong-image</li> <li>bootFailed</li> <li>tooHot</li> <li>booting</li> </ul> <p>A condition of unknown indicates an unsupported interface card. To address this condition, replace the card with a supported card.</p> <p>The operational state of a card must appear as normal for the current status of the card to appear as up.</p> <p>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.</p> <p>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.</p> <p>When your card overheats, the tooHot condition appears in the <b>show card</b> command output. Enter the <b>show fan</b> command to check if your fans have failed.</p> <p>The booting condition indicates that the card has not finished loading necessary image data for internal configuration.</p>

**Table 3-2 Card Properties Window Field Descriptions**

Field	Description
Boot Stage	<p>Boot Stage appears as one of the following:</p> <ul style="list-style-type: none"> <li>• recovery</li> <li>• ipl</li> <li>• ppcboot</li> <li>• fpga</li> <li>• pic</li> <li>• ib</li> <li>• rootfs</li> <li>• kernel</li> <li>• exe</li> <li>• done</li> <li>• none</li> </ul>
Boot Status field	<p>Boot Status may appear as any of the following:</p> <ul style="list-style-type: none"> <li>• upgrading</li> <li>• success</li> <li>• failed</li> <li>• badVersion</li> <li>• badCrc</li> <li>• memoryError</li> <li>• outOfSpace</li> <li>• programmingError</li> <li>• hardwareError</li> <li>• fileNotFound</li> <li>• inProgress</li> <li>• none</li> </ul>
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 <b>Apply</b> .

## 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.  Chassis Manager displays the device ID and version number of the IB chip for each Anafa 2 card in parentheses next to the firmware version. For original Anafa chips, no parenthetical text appears.
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

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 <b>fc</b> to indicate Fibre Channel, <b>en</b> to indicate Ethernet, and <b>ib</b> 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 cards 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	<b>Enable</b> 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 FibreChannel 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.
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

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

Field	Description
Auto Negotiation	<b>Enable</b> check box enables or disables autonegotiation on the port.
Set Port Speed	<b>1G</b> and <b>2G</b> 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 that configure the administrative status of the port.
Oper Status	Displays <b>up</b> 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	2500M, 10G, and 30G radio buttons configure the port speed.
Current Speed	Speed of the port.
Physical State	Physical state of the 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 cards 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.

**Table 3-10 Port Statistics Display Field Descriptions (continued)**

Field	Description
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.

## Configuring a Port Name

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

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Expand <b>Chassis</b> in the Tree frame.  |
| <b>Step 2</b> | Select the <b>Ports</b> branch.<br>The Ports table appears in the View frame. A radio button appears to the left of each table entry. |
| <b>Step 3</b> | Click the radio button of the port to which you want to assign a name.  |
| <b>Step 4</b> | Click <b>Properties</b> .<br>The Port Properties window opens.  |
| <b>Step 5</b> | In the Name field of the Port Properties window, enter a name for the port, and then click <b>Apply</b> .                             |
| <b>Step 6</b> | Click <b>Close</b> to close the Port Properties window.   |
- 

## Enabling or Disabling a Port

To enable or disable a port, follow these steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand the <b>Chassis</b> icon in the Tree frame.  |
| <b>Step 2</b> | Select the <b>Ports</b> branch.<br>The Ports table appears in the View frame. A radio button appears to the left of each table entry.                      |
| <b>Step 3</b> | Click the radio button of the port to which you want to assign a name.   |
| <b>Step 4</b> | Click <b>Properties</b> .<br>The Port Properties window opens.   |
| <b>Step 5</b> | In the Admin Status field of the Port Properties window, click the <b>up</b> (enable) or <b>down</b> (disable) radio button, and then click <b>Apply</b> . |
| <b>Step 6</b> | Click <b>Close</b> 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 to which you want to assign a name.
  - Step 4** Click **Properties**.  
The Port Properties window opens.
  - Step 5** In the Auto Negotiation field of the Port Properties window, click the **Enable** check box to check (enable) or uncheck (disable) it, and then click **Apply**.
  - Step 6** Click **Close** to close the Port Properties window.
- 

## Configuring Port Speed

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 to which you want to assign a name.
  - Step 4** Click **Properties**.  
The Port Properties window opens.
  - Step 5** In the Auto Negotiation field, uncheck the **Enable** check box (if necessary).
  - Step 6** In the Set Port Speed field of the Port Properties window, click a radio button to select a speed, and then click **Apply**.
  - Step 7** Click **Close** to close the Port Properties window.
-

# Viewing Power Supply Status

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 on the power supplies in your device, see your hardware documentation.
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.
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 on the power supplies in your device, see your hardware documentation.
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

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. For more information, see the fan documentation.
Current Status	Displays up if the fan functions properly; otherwise, displays down.
Speed (%)	Speed of the fan in percentage of maximum speed.
Product Version ID	Version of the fan.

## 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. [Table 3-14](#) describes the fields in the Fans 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.
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 Power Supplies 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.

**Table 3-18 Ethernet Management Ports Display Field Descriptions (continued)**

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 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 IB management port.
MTU	Maximum transmission unit of the IB management port.



# Maintenance Tasks

---

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

- [Configuring Basic System Information, page 4-1](#)
- [Configuring System Global Settings, page 4-3](#)
- [Configuring Date and Time Properties, page 4-4](#)
- [Viewing Files in the File System, page 4-5](#)
- [Installing Software Images, page 4-6](#)
- [Importing Configuration Files and Image Files with FTP or SCP, page 4-7](#)
- [Exporting Configuration Files and Log Files with FTP or SCP, page 4-7](#)
- [Customizing the Boot Configuration, page 4-8](#)
- [Backing Up the Running Configuration File, page 4-8](#)
- [Saving a Configuration File, page 4-9](#)
- [Rebooting the Device, page 4-9](#)
- [Configuring Basic Services, page 4-9](#)
- [Viewing RADIUS Servers, page 4-12](#)
- [Viewing TACACS Servers, page 4-15](#)
- [Viewing Authentication Failures, page 4-18](#)
- [Viewing Diagnostic Test Results, page 4-18](#)

## Configuring Basic System Information

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



### 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 UID (select chassis only)	Unique rack-locator ID.

## 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 Technical Support Resource

The technical support e-mail address that you define appears in the System frame when you refresh or restart Chassis Manager. To define a technical support 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 your technical support provider, and then click **Apply**.
- 

## Configuring System Global Settings

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

### 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. Change the system operation mode by doing the following:

- 
- 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, and then click **Apply**.
-

## Enabling InfiniBand Counter Reset

Counters are accumulated by the port\_agent when performance monitoring is enabled (by default, it is disabled). To 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, check the **Enable** check box, and then 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.

### 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**

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

---

## 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: <ul style="list-style-type: none"><li>• config</li><li>• log</li><li>• image</li></ul>
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**.
- 

## 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.
- 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** 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 4-7.

---



---

**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.

---



---

**Note** 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 you into the server.
  - Step 8** Enter your password in the Remote Password field to log you 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.
  - 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

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

Customize the boot configuration to follow these steps:


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

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** (Optional) 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 4-8.
- 
- Step 5** (Optional) Click the **Delete startup configuration** radio button to configure your Server Switch to use the factory-default startup configuration.
- Step 6** 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** Optionally, 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** Click **Reboot**.
- 

## Configuring Basic Services

Configure basic services to facilitate remote access to your device.

## Assigning a DNS Server

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

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand <b>Maintenance</b> in the Tree frame.   |
| <b>Step 2</b> | Expand <b>Services</b> in the Tree frame.  |
| <b>Step 3</b> | Select the <b>General</b> branch.<br>The System Services display appears in the View frame.  |
| <b>Step 4</b> | In the Server 1 field, enter the IP address of the primary DNS server that you want to use.  |
| <b>Step 5</b> | (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. |
| <b>Step 6</b> | In the Domain field, enter the domain to which you want your switch to belong, and then click <b>Apply</b> .                         |
- 

## Enabling or Disabling the FTP Access

To enable FTP transfers to and from your device, follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Expand <b>Maintenance</b> in the Tree frame.  |
| <b>Step 2</b> | Expand <b>Services</b> in the Tree frame.   |
| <b>Step 3</b> | Select the <b>General</b> branch.<br>The System Services display appears in the View frame.                             |
| <b>Step 4</b> | In the FTP Server field, check (enable) or uncheck (disable) the <b>Enable</b> check box, and then click <b>Apply</b> . |
- 

## Enabling or Disabling the Telnet Access

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

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand <b>Maintenance</b> in the Tree frame.   |
| <b>Step 2</b> | Expand <b>Services</b> in the Tree frame.  |
| <b>Step 3</b> | Select the <b>General</b> branch.<br>The System Services display appears in the View frame.                                |
| <b>Step 4</b> | In the Telnet Server field, check (enable) or uncheck (disable) the <b>Enable</b> check box, and then click <b>Apply</b> . |
-

## 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) to accept messages from your device, and then 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 with the local CLI user database only.
localThenRadius	Authenticates user logins with the local CLI user database; upon failure, authenticates with the RADIUS server.
radiusThenLocal	Authenticates user logins with the RADIUS server; upon failure, authenticates with the local CLI user database.
localThenTacacs	Authenticates user logins with the local CLI user database; upon failure, authenticates with the TACACS server.
tacacsThenLocal	Authenticates user logins with the TACACS server; upon failure, authenticates with the local CLI user database.

---

## 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 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 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.
UDP Port	UDP authentication port of the RADIUS server.
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.
Priority	Server priority for use.

---



## 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 <b>Apply</b> 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 <b>Apply</b> 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 <b>Apply</b> 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.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username.  Edit this value and click <b>Apply</b> 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 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.
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 <b>Apply</b> 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 <b>Apply</b> 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 <b>Apply</b> 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.
Max Retries	Number of sequential logins that a user may perform before the server denies access to the username. Edit this value and click <b>Apply</b> 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.

## 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 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 FRU Errors

To view 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. The display lists each FRU and any error messages that apply to the FRU.

---





# InfiniBand Tasks

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

- [Viewing Subnet Managers, page 5-1](#)
- [Viewing InfiniBand Services, page 5-5](#)
- [Viewing InfiniBand Nodes, page 5-7](#)
- [Viewing InfiniBand Ports, page 5-10](#)
- [Viewing Neighboring InfiniBand Devices, page 5-15](#)
- [Viewing IOUs, page 5-17](#)
- [Viewing IOCs, page 5-17](#)
- [Viewing IOC Services, page 5-19](#)

## 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 2.7.0.
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 that the Subnet Manager waits before resending a MAD.
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.

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

Field	Description
Maximum Hop Count	Maximum number of hops considered by Subnet Manager when calculating routes in a subnet.
MadRetries	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.
WaitReportResponse	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 <b>false</b> , the Subnet Manager only sends the Report MADs once; if set to <b>true</b> , 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 <b>false</b> .
SaMadQueueDepth	Size of the SA's internal queue 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.
  - Step 5** Assign a priority value (integer) between 0 and 15 in the Priority field. The higher the integer, the higher the priority.
  - Step 6** (Optional) Enter a key in the Subnet Manager Key field.
  - 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

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.
- 

To configure optional Subnet Manager properties, follow these steps:

- 
- Step 1** (Optional) Enter an integer in the Priority field to configure the priority of the Subnet Manager; the higher the number, the greater the priority.
  - Step 2** (Optional) Enter an integer (1– 268435455) in the Sweep Interval field to configure the sweep interval, in seconds, of the Subnet Manager.
  - Step 3** (Optional) 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 4** (Optional) Enter an integer 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 5** (Optional) Enter an integer in the Master Poll Retries field to configure the number of unanswered polls that cause the standby to identify the master as dead.
  - Step 6** (Optional) Enter an integer value 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 7** (Optional) Enter an integer value in the LID Mask Control field to configure LID mask control on your Subnet Manager.
  - Step 8** (Optional) Enter an integer value between 0 and 20 in the Switch Life Time field.
  - Step 9** (Optional) Enter an integer value between 0 and 20 in the Switch Link HoQ Life field.

- Step 10** (Optional) 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 11** (Optional) 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 12** (Optional) 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 13** (Optional) Enter an integer (256 – 1024) in the SaMadQueueDepth field to configure the size of the SA's internal queue for receiving MADs. The default value is 256.
- Step 14** Click **Apply** to apply your change(s) to your Server Switch.

## Viewing InfiniBand Services

Subnet services provide your InfiniBand fabric with various features, 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

- Step 1** Expand **InfiniBand** in the Tree frame.
- Step 2** Select the **Services** branch.
- The Services table appears in the View frame.
- Step 3** 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.
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

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.
- Step 3** 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.

**Table 5-6**      **Topology Node Properties Window Field Descriptions (continued)**

Field	Description
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 (i.e., 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.



**Table 5-7**      **Topology Node Properties Window Field Descriptions, Switch Properties (continued)**

Field	Description
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, 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 pull-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 5-15](#) or see [Table 5-10](#).

---

## Viewing 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.

---

## 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.
MKey	64-bit management key for this port. See section 14.2.4, Management Key and 3.5.3, Keys, 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 the port router and the rules for local identifiers. See section 4.1.3, Local Identifiers, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.
LID	16-bit base-LID of this port.
Master SM LID	16-bit base LID of the master subnet manager managing this port.
Cap Mask	The capability mask identifies the functions that the host supports. 32-bit bitmask that specifies the supported capabilities of the port. A bit value of 1 (one) indicates a supported capability. The bits are 0, 11-15, 18, 21-31 (Reserved and always 0.), 1 IsSM, 2 IsNoticeSupported, 3 IsTrapSupported, 4 IsResetSupported, 5 IsAutomaticMigrationSupported, 6 IsSLMappingSupported, 7 IsMKeyNVRAM (supports M_Key in NVRAM), 8 IsPKeyNVRAM (supports P_Key in NVRAM), 9 Is LED Info Supported, 10 IsSMdisabled, 16 IsConnectionManagementSupported, 17 IsSNMPTunnelingSupported, 19 IsDeviceManagementSupported, 20 IsVendorClassSupported. Values are expressed in hexadecimal.
Diag Code	16-bit diagnostic code. See section 14.2.5.6.1 Interpretation of Diagcode, InfiniBand Architecture, Vol. 1, Release 1.0, for more information. This field does not currently apply to your device.

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

Field	Description
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.
Link Width Enabled	Enabled link width (bandwidth). The value is an integer that indicates the enabled link-width sets for this port. The value may be as follows: 0 (no state change) <ul style="list-style-type: none"> <li>1 (1x)</li> <li>2 (4x)</li> <li>3 (1x or 4x)</li> <li>8 (12x)</li> <li>9 (1x or 12x)</li> <li>10 (4x or 12x)</li> <li>11 (1x, 4x or 12x)</li> <li>255 (set this parameter to the link-width-supported value)</li> </ul>
Link Width Supported	Supported link width. The value is 1 (1x), 3 (1x or 4x), or 11 (1x, 4x, or 12x).
Link Width Active	Active link width. Used with LinkSpeedActive to determine the link rate between two nodes. The value is 1 (1x), 2 (4x), or 8 (12x).
Link Speed Supported	Supported link speed. The value is 1 (2.5 Gbps).
State	A higher form of addressing than PhyState, 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.
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), 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, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.

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

Field	Description
LMC	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, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.
Link Speed Active	Speed of an active link. The value is 1 (2.5 Gbps).
Link Speed Enabled	Maximum speed that the link is capable of handling. The value is 0 (No state change), 1 (2.5 Gbps), or 3 (value derived from link-speed-supported).
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.
VL Cap	Maximum range of data virtual lanes supported by this port. The value is v10, v10ToV11, v10ToV13, v10ToV17, or v10ToV114. 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.
VL 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, 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, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.
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 256, 512, 1024, 2048, or 4096
VL Stall Count	Number of sequentially dropped packets at which the port enters a VLStalled state. The virtual lane exits the VLStalled state (8 * HLL) units after entering it. See section 18.2.5.4, Transmitter Queuing, InfiniBand Architecture, Vol. 1, Release 1.0, 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.

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

Field	Description
Oper VL	Administrative limit for the number of virtual lanes allowed to the link. Do not set this above the VL-cap value. The value is v10, v10-V11, v10-V13, v10-V17, or v10-V114.
In Part Enforce	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 Part Enforce	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 Enforce	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 Enforce	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, InfiniBand 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), 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, 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, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.
Subnet Timeout	Maximum propagation delay allowed for this port to reach any other port in the subnet. This value also affects the maximum rate at which traps can be sent from this port. Delay is affected by switch configuration. This parameter, along with resp-time is used to determine the interval to wait for a response to a request before taking other action. Duration is calculated as $(4.096 \text{ ms} * 2^{\text{SubnetTimeout}})$ .
Response Time	Maximum time allowed between the port reception of a subnet management packet and the transmission of the associated response. See section 13.4.6.2, Timers and Timeouts, InfiniBand Architecture, Vol. 1, Release 1.0, for more information.

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

Field	Description
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, 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

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.
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.
Close	Closes the window.
Help	Opens online help.

---



# 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

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.

**Table 5-13** *IOCs Display Field Descriptions (continued)*

Field	Description
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.

**Table 5-14** *IOC Properties Window Field Descriptions (continued)*

Field	Description
Controller Op Cap Mask	Integer value (from 8 cumulative bits) between 1 and 255 that represents the operation type(s) that the IOC supports: <ul style="list-style-type: none"> <li>• bit 0: ST; Send Messages To IOCs</li> <li>• bit 1: SF; Send Messages From IOCs</li> <li>• bit 2: RT; RDMA Read Requests To IOCs</li> <li>• bit 3: RF; RDMA Read Requests From IOCs</li> <li>• bit 4: WT; RDMA Write Requests To IOCs</li> <li>• bit 5: WF; RDMA Write Requests From IOCs</li> <li>• bit 6: AT; Atomic Operations To IOCs</li> <li>• bit 7: AF; Atomic Operations From IOCs</li> </ul>
Service Entries	Number of services that the IOC provides.

## Viewing 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.
Close	Closes the window.
Help	Opens context-sensitive online help.



## Ethernet Tasks

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

- [Viewing Bridge Groups, page 6-1](#)
- [Viewing Bridge Subnets, page 6-4](#)
- [Viewing Bridge Forwarding, page 6-6](#)
- [Viewing Redundancy Groups, page 6-7](#)
- [Viewing Trunk Groups, page 6-10](#)

### 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.
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.

## 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.
Broadcast Forwarding	Displays a checked box when broadcast forwarding runs.
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.
Broadcast Forwarding Mode	Active broadcast forwarding mode.
IP Multicast Mode	Active IP multicast mode.
Loop Protection Method	Displays the loop protection method of the group.
IP Multicast	Displays a checked box when IP multicasting runs.
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.

## Adding Bridge Groups

To create a new bridge group, follow these steps:

- 
- |                |  |
|----------------|--|
| <b>Step 1</b>  | Expand <b>Ethernet</b> in the Tree frame.  |
| <b>Step 2</b>  | Select the <b>Bridge Groups</b> branch.<br>The Bridge Groups table appears in the View frame.  |
| <b>Step 3</b>  | Click <b>Add</b> .<br>The Add Ethernet Bridge Group window appears.  |
| <b>Step 4</b>  | Enter a bridge group ID number in the ID field.  |
| <b>Step 5</b>  | Click the <b>none</b> radio button or the <b>one</b> radio button in the Loop Protection Method field to choose a protection method. |
| <b>Step 6</b>  | (Optional) Check the <b>Enable</b> check box in the IP Multicast field to enable IP multicasting.                                    |
| <b>Step 7</b>  | Select a port from the Ethernet Port pull-down menu.   |
| <b>Step 8</b>  | Enter a virtual LAN in the Vlan field.   |
| <b>Step 9</b>  | Select an IB gateway port from the IB Port pull-down menu.   |
| <b>Step 10</b> | (Optional) Enter a partition key in the IB P_KEY field.  |
| <b>Step 11</b> | Click <b>Apply</b> .   |
- 

## Configuring Bridge Groups

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

- 
- |                |   |
|----------------|---|
| <b>Step 1</b>  | Expand the <b>Ethernet</b> icon in the Tree frame.  |
| <b>Step 2</b>  | Select the <b>Bridge Groups</b> branch.<br>The Bridge Groups table appears in the View frame.   |
| <b>Step 3</b>  | Click the radio button next to the bridge group whose properties you want to view, and then click <b>Properties</b> .<br>The Ethernet Chassis Manager window opens. |
| <b>Step 4</b>  | (Optional) Enter a name for the bridge group in the Name field.   |
| <b>Step 5</b>  | (Optional) Enter the IP address of the next Ethernet hop of the bridge group in the Ethernet Next Hop field.  |
| <b>Step 6</b>  | (Optional) Enter the IP address of the next destination for packets that enter from the IB fabric in the IB Next Hop field.   |
| <b>Step 7</b>  | (Optional) Check (or uncheck) the <b>Enable</b> check box in the Broadcast Forwarding field.  |
| <b>Step 8</b>  | (Optional) Enter an integer value in the Redundancy Group ID field.   |
| <b>Step 9</b>  | (Optional) Enter an integer value in the Admin Failover Priority field.   |
| <b>Step 10</b> | (Optional) Click the <b>none</b> radio button or <b>one</b> radio button in the Loop Protection Method field.   |
| <b>Step 11</b> | (Optional) Check (or uncheck) the <b>Enable</b> check box in the IP Multicast field.  |

- Step 12** (Optional) Select a port from the Ethernet Port pull-down menu.
- Step 13** (Optional) Enter a virtual LAN ID in the Vlan field.
- Step 14** (Optional) Select a gateway port from the IB Port pull-down menu.
- Step 15** (Optional) Enter a partition key in the IB P\_KEY field.
- Step 16** Click **Apply**.
- 

## Deleting Bridge Groups

To delete 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 that you want to delete, and then click **Delete**.
- 

## 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**.
-

## 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 <b>eth</b> for IP and <b>ib</b> 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 a bridge subnet, 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**.
- 

## 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.

---

## 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.
  - Step 8** (Optional) Check the **Enable** check box in the Ip Multicast Mode field.
  - Step 9** 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 whose properties you want to view.
  - Step 4** Click **Delete**.
-

## Viewing 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	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.
Action	Provides a pull-down menu of actions to execute with the group.
Result	Result of the action that you apply in the Action field.
Broadcast Forwarding Mode	Displays a checked or unchecked <b>Enable</b> check box.
Ip Multicast Mode	Displays a checked or unchecked <b>Enable</b> check box.

# 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	<p>Distribution type of the trunk group. This field displays one of the following types:</p> <ul style="list-style-type: none"> <li>• <b>srcMac</b> 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.</li> <li>• <b>dstMac</b> 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.</li> <li>• <b>srcDstMac</b> bases load distribution on the MAC address of the source logic gate (XOR) destination.</li> <li>• <b>srcIp</b> 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.</li> <li>• <b>dstIp</b> 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.</li> <li>• <b>srcDstIp</b> bases load distribution on the IP address of the source logic gate (XOR) destination.</li> </ul>
Trunk Group Enabled	Displays a checked <b>Enable</b> check box to indicate an active trunk group.
MTU	Maximum transmission unit (MTU) of the group.
MAC Address	MAC address of the trunk group.
IfIndex	Interface index of the trunk group.

## 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**.
- 

## Viewing Trunk Group Properties

To view the properties of 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 trunk group whose properties you want to view, and then click **Properties**.  
The Ethernet Trunk Group Properties window opens. [Table 6-8](#) describes the fields in this window.

**Table 6-8** Ethernet Trunk Group Properties Window 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.

**Table 6-8 Ethernet Trunk Group Properties Window Field Descriptions (continued)**

Field	Description
Distribution Type	<p>Distribution type of the trunk group. This field displays one of the following types:</p> <ul style="list-style-type: none"> <li>• <b>srcMac</b> 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 channel.</li> <li>• <b>dstMac</b> 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 channel.</li> <li>• <b>srcDstMac</b> bases load distribution on the MAC address of the source logic gate (XOR) destination.</li> <li>• <b>srcIp</b> 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 channel.</li> <li>• <b>dstIp</b> 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 channel.</li> <li>• <b>srcDstIp</b> bases load distribution on the IP address of the source logic gate (XOR) destination.</li> </ul>
Trunk Group Enabled	Displays a checked <b>Enable</b> 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.

## 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**.
-





## FibreChannel Tasks

---

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

- [Configuring Global ITL Attributes, page 7-1](#)
- [Viewing SRP Hosts \(Initiators\), page 7-2](#)
- [Viewing FibreChannel Targets, page 7-6](#)
- [Viewing FibreChannel LUNs, page 7-9](#)
- [Viewing ITs, page 7-12](#)
- [Viewing ITLs, page 7-13](#)
- [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 *FibreChannel 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 **FibreChannel** 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:
- (Optional) Click 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.
  - (Optional) Click 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 between FibreChannel 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 FibreChannel 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 SRP Hosts (Initiators)

To view the SRP hosts that connect to your device and, with your Server Switch, behave as FibreChannel initiators, follow these steps:

**Step 1** Expand **FibreChannel** 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	Port(s) 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 **FibreChannel** 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	Port(s) 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 key(s) 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 <b>Apply</b> .
Result	Displays the result of the action that you performed with the pull-down menu in the Action field.

## 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 **FibreChannel** 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 **FibreChannel** 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” 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 **FibreChannel** 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, see the [“Viewing ITLs” section on page 7-13](#) or see [Table 7-10](#).
- 

## Adding SRP Host

To add a SRP host to the configuration file, follow these steps:

- 
- Step 1** Expand **FibreChannel** 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 SRP Host

To delete an SRP host, follow these steps:

- 
- Step 1** Expand the **FibreChannel** 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 **FibreChannel** 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 FibreChannel Targets

To view the FibreChannel targets in the configuration file of your Server Switch, follow these steps:

- 
- Step 1** Expand the **FibreChannel** 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. <b>Note</b> 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 <b>nlport</b> to indicate a virtual FC port, or <b>down</b> to indicate a faulty connection.

---



## Viewing FibreChannel Target Properties

To view the properties of a FibreChannel target, follow these steps:

- Step 1** Expand **FibreChannel** 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	FibreChannel 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 FibreChannel 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 <b>down</b> and <b>nlPort</b> radio buttons assign a connection type to the target.
Description	User-assigned target description. <b>Note</b> If no user has assigned a description, a default description appears.
Service Name	Name of the service to associate with the WWPN.
Apply	Applies the changes that you make in the window.
Reset	Resets the fields in the window to match the properties of the target.
Close	Closes the window. If you close the window before you apply changes, Chassis Manager makes no changes to the target.
Help	Opens online help.

## Configuring FibreChannel Target Properties

To configure the properties of a FibreChannel target, follow these steps:

- 
- Step 1** Expand **FibreChannel** 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 **FibreChannel** 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” 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 **FibreChannel** 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” section on page 7-13](#) or see [Table 7-10](#).
- 

## Viewing FibreChannel LUNs

To view the logical units (FC storage disks) in the configuration file of your Server Switch, follow these steps:

- 
- Step 1** Expand **FibreChannel** 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 port(s) through which your Server Switch accesses the LU.

---

## Viewing FibreChannel LUN Properties

To view FibreChannel LUN properties, follow these steps:

- Step 1** Expand **FibreChannel** 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 <b>random</b> radio button and <b>sequential</b> 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.
Min IO Timeout	Maximum amount of time that elapses before a SRP request times out.
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 FibreChannel LUN Properties

To configure FibreChannel LUN properties, follow these steps:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand <b>FibreChannel</b> in the Tree frame.  |
| <b>Step 2</b> | Select the <b>Logical Units</b> branch.<br><br>A Logical Units table that includes all LUs in your configuration file appears in the View frame.         |
| <b>Step 3</b> | Click the radio button next to the LUN whose properties you want to view, and then click <b>Properties</b> .<br><br>The SRP LUN Properties window opens. |
| <b>Step 4</b> | (Optional) Enter a description in the Description field.   |
| <b>Step 5</b> | (Optional) Enter an integer value in the Hi Mark field.  |
| <b>Step 6</b> | (Optional) Enter an integer value in the Max Retry field.  |
| <b>Step 7</b> | (Optional) Enter an integer value in the Min IO Timeout field.   |
| <b>Step 8</b> | (Optional) Click a radio button in the Dynamic Pathing field.  |
| <b>Step 9</b> | Click <b>Apply</b> , and then click <b>Close</b> .   |
- 

## 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:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Expand <b>FibreChannel</b> in the Tree frame.  |
| <b>Step 2</b> | Select the <b>Logical Units</b> branch.<br><br>A Logical Units table that includes all FC targets that connect to the chassis appears in the View frame.   |
| <b>Step 3</b> | Click the radio button next to the LUN whose ITLs you want to view.  |
| <b>Step 4</b> | Select <b>Show ITL Policies</b> from the Show Options pull-down menu.<br><br>The <b>ITLs</b> display appears in the View frame but lists only ITLs that include the LUN that you selected. For more information, see the <a href="#">“Viewing ITLs” section on page 7-13</a> or see <a href="#">Table 7-10</a> . |
-

# Viewing ITs

To view Initiator-Target (IT) pairs on your Server Switch, follow these steps:

**Step 1** Expand **FibreChannel** 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 port(s) 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 **FibreChannel** 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 port(s) 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.

**Table 7-9 SRP IT Properties Window Field Descriptions (continued)**

Field	Description
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 todo ITL logins for this IT without the participation of the initiator's HBA.  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 <b>Discover ITLs</b> from the Action pull-down menu and then click <b>Apply</b> .

## Viewing ITLs

To view Initiator-Target-LUN (ITL) properties, follow these steps:

**Step 1** Expand **FibreChannel** 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	FibreChannel 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 **FibreChannel** 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.
FC LUN ID	FibreChannel ID of the disk or tape in the target. The ID of the first LUN is always <b>00:00:00:00:00:00:00:00</b> , 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 <b>00:00:00:00:00:00:00:00</b> , 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 port(s) 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 **FibreChannel** 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 FibreChannel interface gateway(s).
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 FibreChannel 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 FibreChannel interface gateway(s).
SRP Errors	Total number of SRP errors encountered on the FibreChannel interface gateway(s).
FCP Initiated IOs	Total number of I/O responses by the FibreChannel device to SRP initiator requests.
FCP Commands Completed	Total number of FCP commands completed on the FibreChannel interface gateway(s).
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 FibreChannel interface gateway(s).
FCP Errors	Total number of FCP errors encountered on the FibreChannel interface gateway(s).





---

## A

access privileges [2-7](#)  
admin status  
    configuring, card [3-7](#)  
authentication [4-11](#)  
authentication failures [1-4](#)  
auto-negotiation [3-14](#)  
auto-negotiation, configuring [3-14, 3-19](#)

---

## B

backing up configuration files [4-8](#)  
backplane, viewing [3-18](#)  
baud rate [3-19](#)  
boot configuration, setting [4-8](#)  
bridge groups  
    adding [6-3](#)  
    configuring [6-3](#)  
    deleting [6-4](#)  
    properties [6-2](#)  
    viewing [6-1](#)  
bridging, port [3-11](#)

---

## C

cards  
    inventory [3-6](#)  
    viewing [3-1](#)  
    viewing properties [3-4](#)  
card test results [4-19](#)  
CLI authentication [4-11](#)  
configuration files

    backing up [4-8](#)  
    boot config, setting [4-8](#)  
    exporting [4-7](#)  
    importing [4-7](#)  
    saving [4-9](#)  
current status  
    card [3-4](#)  
    ports [3-20](#)

---

## D

data bits [3-19](#)  
date, configuring [4-4](#)  
disable  
    port [3-13](#)  
DNS [4-10](#)  
DNS system service [1-4](#)  
documentation  
    conventions [x](#)  
    organization [ix](#)

---

## E

enable  
    port [3-13](#)  
encryption key  
    TACACS [4-16](#)  
encryption key, configuring [4-13, 4-16](#)  
exporting  
    configuration files [4-7](#)  
    log files [4-7](#)

---

**F**

fan

- test results [4-19](#)

fan status [3-17](#)

files, deleting [4-6](#)

file system

- deleting files [4-6](#)
- viewing [4-5](#)

filter indicator [2-7](#)

frames, GUI

- Tree [1-2](#)
- View [1-6](#)

Fru errors [1-4](#)

FRU number, card [3-5](#)

FRU test results [4-20](#)

FTP [4-10](#)

FTP system service [1-4](#)

---

**G**

gateway ports, internal [3-7](#)

global ITL

- attributes [7-1](#)
- policies [7-1](#)
- statistics [7-15](#)

---

**H**

Hop Count [5-3](#)

HoQ life [5-2](#)

hosts

- adding [7-5](#)
- configuring [7-6](#)
- deleting [7-5](#)
- ITLs [7-5](#)
- ITs [7-4](#)
- properties [7-3](#)
- viewing [7-2](#)

- WWPNs [7-4](#)

host-target-LUN policies [7-13](#)

host-target-LUN properties [7-14](#)

host-target policies [7-12](#)

host-target properties [7-12](#)

HTTP [1-4](#)

HTTP authentication failures [1-4](#)

---

IB counter reset [4-3](#)

image files, importing [4-7](#)

importing

- configuration files [4-7](#)
- image files [4-7](#)

InfiniBand nodes

- viewing [5-7](#)

Infiniband Nodes

- properties [5-7](#)

InfiniBand ports

- properties [5-11](#)
- viewing [5-10](#)

initiators

- adding [7-5](#)
- configuring [7-6](#)
- deleting [7-5](#)
- ITLs [7-5](#)
- ITs [7-4](#)
- properties [7-3](#)
- viewing [7-2](#)
- WWPNs [7-4](#)

installing software [4-6](#)

internal gateway ports [3-7](#)

IOCs

- properties [5-18](#)
- services [5-19](#)
- viewing [5-17](#)

IOUs [5-17](#)

IP addresses

Ethernet management port [3-20](#)

## IT

policies [7-12](#)

properties [7-12](#)

## ITL

global attributes [7-1](#)

global policies [7-1](#)

policies [7-13](#)

properties [7-14](#)

## L

launching Chassis Manager [2-2](#)

location [4-3](#)

locator [2-6](#)

log files, exporting [4-7](#)

logging out of chassis manager [2-6](#)

## LUNs

configuring [7-11](#)

ITLs [7-11](#)

properties [7-10](#)

viewing [7-9](#)

## M

MAC (media access control) [3-19](#)

MAC Address [3-9](#)

MadRetries [5-5](#)

management ports, viewing [3-19](#)

Max Retries [4-16, 4-17](#)

max retry, configuring for RADIUS [4-13, 4-16](#)

media access control (MAC) address [3-19](#)

MTU [3-9](#)

## N

### name

configuring port names [3-13](#)

file [4-5](#)

switch name [4-2](#)

neighbor properties, viewing [5-16](#)

neighbors, InfiniBand [5-10, 5-15](#)

net mask, ports [3-20](#)

node neighbors, viewing [5-10](#)

node ports, viewing [5-9](#)

### nodes

properties [5-7](#)

viewing [5-7](#)

viewing neighbors [5-10](#)

viewing ports [5-9](#)

NodeTimeout [5-5](#)

NTP servers, assigning [4-5](#)

## O

operational state, card [3-4](#)

## P

parity [3-19](#)

### PCA

assembly number

card [3-5](#)

serial number

card [3-5](#)

port bridging properties [3-11](#)

### ports

administrative status [3-20](#)

auto-negotiation [3-14](#)

bridging properties [3-11](#)

configure properties [3-12](#)

current status [3-20](#)

enabling and disabling [3-13](#)

gateway [3-20](#)

IP address [3-20](#)

management ports [3-19](#)

- name, configuring [3-13](#)
- net mask [3-20](#)
- node ports [5-9](#)
- properties [3-8](#)
- speed, configuring [3-14](#)
- view all [3-8](#)
- view internal gateway [3-7](#)
- ports, InfiniBand
  - viewing [5-10](#)
- Ports, InfiniBand Ports
  - properties [5-11](#)
- POST errors [1-4](#)
- POST tests [4-19, 4-20](#)
- power supply
  - test results [4-20](#)
- power supply status [3-15](#)
- prepare your switch [2-1](#)
- prerequisites [2-1](#)
- printed circuit assembly (PCA) [3-5](#)

## R

### RADIUS

- adding [4-14](#)
- configuring [4-13](#)
- deleting [4-14](#)
- viewing [4-12](#)

### RADIUS server

- configuring encryption key [4-13, 4-16](#)
- configuring max retry value [4-13, 4-16](#)
- configuring timeout [4-13, 4-16](#)
- configuring UDP port [4-13, 4-16](#)

### RADIUS servers [1-4](#)

### RADIUS system service [1-4](#)

- rebooting [4-9](#)
- reloading [4-9](#)

## S

- SA MAD Queue Depth [5-3, 5-5](#)
- saving configuration files [4-9](#)
- serial number [3-5](#)
- services (basic), configuring [4-9](#)
- setup [2-1](#)
- slot ID [3-4](#)
- software, installing [4-6](#)
- speed, port speed [3-14](#)
- SRP Hosts
  - adding [7-5](#)
  - configuring [7-6](#)
  - deleting [7-5](#)
  - ITLs [7-5](#)
  - ITs [7-4](#)
  - properties [7-3](#)
  - viewing [7-2](#)
  - WWPNs [7-4](#)
- starting Chassis Manager [2-2](#)
- statistics, global ITL [7-15](#)
- status
  - viewing [2-8](#)
- stop bits [3-19](#)
- subnet manager
  - adding [5-3](#)
  - configuring [5-4](#)
  - deleting [5-4](#)
  - properties [5-2](#)
  - viewing [5-1](#)
- subnet services
  - properties [5-6](#)
  - viewing [5-5](#)
- switch configuration [2-1](#)
- SYSLOG [4-11](#)
- Syslog system service [1-4](#)
- system operating mode [4-3](#)

---

**T**

TACACS servers [1-4](#)

- adding [4-17](#)
- configuring [4-16](#)
- deleting [4-17](#)
- viewing [4-15](#)

TACACS system service [1-4](#)

targets

- configuring [7-8](#)
- ITLs [7-9](#)
- ITs [7-8](#)
- properties [7-7](#)
- viewing [7-6](#)

telnet [4-10](#)

TELNET system service [1-4](#)

temperature sensor status [3-18](#)

tiered locator [2-6](#)

time, configuring [4-4](#)

timeout, configuring for RADIUS server [4-13, 4-16](#)

Tree frame [1-2](#)

trunk groups

- adding [6-11](#)
- configuring [6-12](#)
- deleting [6-13](#)
- properties [6-11](#)
- viewing [6-10](#)

type, card [3-4](#)

---

**U**

UDP authentication [4-16](#)

UDP port, configuring [4-13, 4-16](#)

---

**V**

VFrame [4-3](#)

View frame [1-6](#)

---

**W**

WaitReportResponse [5-5](#)

