



Cisco SFS InfiniBand Fibre Channel Gateway User Guide

Release 2.8.0

June, 2007

Americas Headquarters

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

Text Part Number: OL-12943-01

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

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

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

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

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

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

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

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

Cisco SFS InfiniBand Fibre Channel Gateway User Guide
© 2006–2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Audience vii

Organization vii

Conventions viii

Related Documentation ix

Obtaining Documentation, Obtaining Support, and Security Guidelines ix

CHAPTER 1

About the Fibre Channel Gateway 1-1

Introducing the Fibre Channel Gateway 1-1

Terms and Concepts 1-2

Hardware Features 1-4

 Bandwidth and Speed 1-4

 Maintenance 1-4

Software Features 1-4

 Redundancy and High Availability 1-5

 Access Control 1-5

 Speed 1-6

 Topologies 1-6

How the Fibre Channel Gateway Works 1-6

Initiator-Target-LUN (ITL) Groups 1-8

 Initiators 1-8

 Targets 1-9

 LUNs 1-9

CHAPTER 2

Fibre Channel Gateway High Availability 2-1

Redundant Topologies 2-1

Load Balancing 2-3

Dynamic Gateway Failover 2-3

 Recovering from a Fibre Channel Gateway Failure or Disconnect 2-3

 Redistributing Traffic and SRP Connections 2-4

CHAPTER 3**Global Attributes 3-1**

- About Global Attributes 3-1
- Configuring Global Attributes 3-1
 - Using Element Manager 3-1
 - Using the CLI 3-4
- Viewing Global Attributes 3-10
 - Viewing with the Element Manager 3-11
 - Viewing with the CLI 3-12

CHAPTER 4**Installing and Configuring Hardware 4-1**

- Installing a Fibre Channel Gateway 4-1
 - Connecting to a Fibre Channel SAN 4-1
- Removing a Fibre Channel Gateway 4-2
- Interpreting LEDs 4-2

CHAPTER 5**Using the Fibre Channel Gateway 5-1**

- Configuring a Fibre Channel Gateway 5-1
 - Configuring a New Fibre Channel Gateway 5-2
 - Updating Existing Configurations 5-2
- Administering the Fibre Channel Gateway 5-2
 - Bringing Up a Card 5-2
 - Bringing Down a Card 5-4
 - Bringing Up a Port 5-4
- Configuring Initiators 5-5
- Configuring Targets and LUNs 5-6
- Configuring Initiator-Target Pairs 5-6
 - Configuring IT Pair Mode for Persistent Binding 5-6
- Configuring ITLs 5-7
 - Configuring ITLs with Element Manager while No Global Policy Restrictions Apply 5-7
 - Configuring ITLs with Element Manager while Global Policy Restrictions Apply 5-9
 - Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1 5-10
 - Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 2 5-15
 - Configuring ITLs with Custom WWNNs and WWPNS 5-19
- Configuring Port Access on Existing ITs and ITLs 5-21
 - Granting Port Access with Element Manager 5-21
 - Denying Port Access with Element Manager 5-22
 - Granting Port Access with the CLI 5-23
 - Denying Port Access with the CLI 5-24

Viewing Port Access Settings	5-25
Viewing Port Mask Settings with Element Manager	5-25
Viewing Port Masking Settings with the CLI	5-25
Configuring LUN Access on Existing ITLs	5-27
Granting LUN Access on an ITL with Element Manager	5-27
Denying LUN Access on an ITL with Element Manager	5-27
Granting LUN Access on an ITL with the CLI	5-28
Denying LUN Access on an ITL with the CLI	5-30
Viewing LUN Access Settings	5-31
Viewing LUN Access with Element Manager	5-31
Viewing LUN Access with the CLI	5-31
Configuring Individual ITL Attributes	5-32
Configuring ITL I/O High Mark	5-33
Configuring ITL Maximum Retries	5-34
Configuring ITL Minimum I/O Timeout	5-35
Configuring Dynamic Path Affinity	5-36
Configuring Dynamic Load Balancing	5-37
Configuring Dynamic Failover	5-38
Configuring ITL Description	5-39
Gateway Grouping	5-40
WWPN Overload with Auto Binding	5-41
WWPN Limits with Gateway Grouping	5-41
Manually Configuring with the CLI	5-41

CHAPTER 6

ITLs and Zoning	6-1
Introduction	6-1
Adding Unzoned Initiators (Fibre Channel Gateway Ports)	6-1
Adding Initiators	6-2
Verify Zoning	6-2
Configuring RAID Arrays	6-2

CHAPTER 7

Configuring PowerPath with a Server Switch	7-1
Topology	7-1
Setup	7-1
Introduction	7-2
Configuring Fibre Channel Gateway Access to Clariion	7-2
Configuring SRP Host Access to Clariion	7-11

CHAPTER 8

Configuring Hitachi Storage 8-1

- Sample Topology 8-1
- Installing and Configuring the Storage Application (DAMP 3) 8-1
- Connecting the Array to the Fibre Channel Gateway 8-4
- Using Host Group Security 8-6
- Managing Host Groups 8-6
 - Adding WWN 8-8
- Configuring a RAID Group 8-10
- Adding LUs to a RAID Group 8-13
- Making LUs Visible to Hosts 8-14

CHAPTER 9

LUN Remapping 9-1

- Introduction 9-1
- Creating an SRP LUN for a Fibre Channel LUN 9-1
 - Using the CLI 9-1
 - Using Chassis Manager 9-2
 - Using Element Manager 9-2
- Configuration Example 9-3

CHAPTER 10

Monitoring Storage Traffic 10-1

- Introduction 10-1
- Global Statistics 10-1
 - Global Tab Field Descriptions 10-1
 - Viewing Global Statistics 10-2
- SRP/FCP Statistics 10-3
 - Viewing SRP/FCP Statistics 10-4
- Fibre Channel Gateway Statistics 10-4
 - Viewing Statistics for a Specific Gateway 10-4
- Viewing ITL Statistics 10-5

INDEX



Preface

This preface describes who should read the *Cisco InfiniBand Fibre Channel Gateway User Guide*, how it is organized, and its document conventions. It contains the following sections:

- [Audience, page vii](#)
- [Organization, page vii](#)
- [Conventions, page viii](#)
- [Related Documentation, page ix](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page ix](#)

Audience

The intended audience is the administrator responsible for configuring and managing Fibre Channel gateways and related software and equipment. It is expected that the user has experience working with equipment such as server switches, the Subnet Manager, Fibre Channel gateways, Host Channel Adapters, and software drivers.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	About the Fibre Channel Gateway	Introduces the Fibre Channel gateway, its key terms and concepts, and its hardware and software features.
Chapter 2	Fibre Channel Gateway High Availability	Provides a sample topology for Fibre Channel gateways in an HA environment and describes failover behavior.
Chapter 3	Global Attributes	Describes how to configure global attributes by using the CLI or Element Manager.
Chapter 4	Installing and Configuring Hardware	Provides steps for installing and uninstalling Fibre Channel gateways.

Chapter	Title	Description
Chapter 5	Using the Fibre Channel Gateway	Provides steps for configuring and administering a Fibre Channel gateway.
Chapter 6	ITLs and Zoning	Provides steps for adding ITLs and zones.
Chapter 7	Configuring PowerPath with a Server Switch	Provides an example topology and instructions for configuring PowerPath.
Chapter 8	Configuring Hitachi Storage	Provides steps for configuring and using an Hitachi storage array.
Chapter 9	LUN Remapping	Provides steps for mapping a Fibre Channel LUN to an SRP LUN.
Chapter 10	Monitoring Storage Traffic	Provides steps for monitoring storage traffic with Element Manager.

Conventions

This document uses the following conventions:

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

Convention	Description
< >	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 related to the Fibre Channel Gateway, see the following documents:

- *Cisco SFS Product Family Command Reference*
- *Cisco SFS Product Family Chassis Manager User Guide*
- *Cisco SFS Product Family Element Manager User Guide*
- *Cisco VFrame InfiniBand Site Planning and Preparation Guide*
- *Cisco VFrame InfiniBand Director User Guide*
- *Cisco VFrame InfiniBand Director Third Party Integration Guide*
- *InfiniBand Hardware Installation and Cabling Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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



CHAPTER 1

About the Fibre Channel Gateway

This chapter includes the following sections:

- [Introducing the Fibre Channel Gateway, page 1-1](#)
- [Terms and Concepts, page 1-2](#)
- [Hardware Features, page 1-4](#)
- [Software Features, page 1-4](#)
- [How the Fibre Channel Gateway Works, page 1-6](#)
- [Initiator-Target-LUN \(ITL\) Groups, page 1-8](#)

Introducing the Fibre Channel Gateway

The Fibre Channel gateway expansion module ([Figure 1-1](#)) connects your server switch to Fibre Channel storage area networks (SANs). The gateway associates a dynamically-generated world-wide node name (WWNN) and associated world-wide port names (WWPNs) with each connected InfiniBand (IB) host, or initiator, to provide seamless connectivity between Fibre Channel and IB networks. Because the gateway creates Fibre Channel-compatible identifiers for IB elements, you can manage your storage without any changes to your current SAN management tools and practices.

Figure 1-1 *Fibre Channel Gateway Expansion Module*

182970

Terms and Concepts

This book refers to a number of terms, concepts, and identifiers that apply to the Fibre Channel gateway and the elements that interact with the gateway. [Table 1-1](#) presents and defines key Fibre Channel gateway terms and concepts.

Table 1-1 *Fibre Channel Gateway Terms and Concepts*

Term	Description
auto-bind	The auto-bind feature of the Fibre Channel gateway dynamically assigns WWNNs and WWPNNs to new initiators. When you configure an initiator, you can manually configure these values, but you might create duplicate values that create network conflicts. The auto-bind feature creates unique WWNNs and WWPNNs to save you time and prevent network conflicts. You must omit the auto-bind feature when you configure initiators if you want to enable gateway grouping. For details about gateway grouping, see “Gateway Grouping” section on page 5-40.
initiator	Your host, Host Channel Adapter (HCA), and server switch emulate a Fibre Channel-attached host, or initiator. The HCA and host drivers render the host SCSI RDMA Protocol (SRP)-capable. For the purposes of this document, the term “initiator” refers to an SRP host.

Term	Description
IT	An initiator-target pair (IT) represents a connection from an SRP host to a storage device target port through a Fibre Channel gateway.
ITL	ITLs serve as the paths between InfiniBand (IB) hosts and Fibre Channel (FC) storage. ITLs consist of an initiator, a target, a logical unit (LU), and the switches between them.
logical unit (LU)	A logical unit is an absolute identifier for a partition, disk, or tape on a Fibre Channel storage device. A given LU identifies one specific storage unit. Your Fibre Channel gateway maps LUs to LUNs, and then your hosts use the LUN identifier to access storage.
logical unit number (LUN)	Each logical unit number, or LUN, identifies a Fibre Channel storage unit. LUNs are not absolute identifiers. Up to 4 different LUNs can represent the same LU. Your Fibre Channel gateway automatically assigns LUNs to LUs. LUNs are initiator-side identifiers. Initiators must be able to see LUNs to write information to the LUs that the LUNs represent.
path affinity	The path affinity feature of the Fibre Channel gateway locks a storage connection to a path for the duration of data transfer to increase speed and efficiency.
random device	A random device is a storage device with LUs that can be accessed randomly (non-sequentially). RAID devices and JBODs qualify as random devices.
sequential device	A sequential device is a storage device with LUs that can only be accessed sequentially. Tape devices qualify as sequential devices. The Fibre Channel gateway lets you configure separate connection defaults for random devices and sequential devices. For instance, because tape (sequential) devices may require more time to access data, you may want to extend time-out values. You can configure random and sequential configuration options when you configure global attributes and ITLs.
service name	A service name is an identifier for a Fibre Channel feature. Service names apply to all Fibre Channel components. The Fibre Channel gateway dynamically creates service names for IB components.
SRP host	The term “SRP host” means the same thing as <i>initiator</i> (above), but it emphasizes the fact that, in an ITL, it is a host that runs SRP communicates with Fibre Channel storage devices.
target	A target is a Fibre Channel storage device. In this document, “target” refers to the <i>port</i> on the storage device through which initiators access disks or tapes.
transparent topology emulation	The transparent topology emulation feature of the Fibre Channel gateway assigns Fibre Channel identifiers to all IB elements, so your SAN can access IB elements as though they were Fibre Channel devices. Transparent topology emulation eliminates any need for you to make changes to your SAN for it to communicate with your IB fabric.
world-wide node name (WWNN)	World-wide node names serve as Fibre Channel identifiers for hosts in the SAN. The Fibre Channel gateway dynamically associates WWNNs with SRP hosts. The Fibre Channel gateway also assigns a WWNN to itself.
world-wide port name (WWPN)	World-wide port names serve as Fibre Channel identifiers for ports in the SAN. When you configure an SRP host (initiator), the Fibre Channel gateway creates a WWPN for every initiator/Fibre Channel gateway-port combination.

Hardware Features

Fibre Channel gateways add bandwidth and speed to your environment.

Bandwidth and Speed

Each port on the Fibre Channel gateway provides up to 2 Gbps of bandwidth. You can configure the ports on a card to run at either 1 Gbps or 2 Gbps.

**Note**

Although you can configure the ports individually, both ports must run at the same speed.

**Note**

If the speeds of the ports on a gateway do not match, the gateway cannot run traffic. Be sure to set both ports to the same speed. For more information, refer to the **speed** command in the *Cisco SFS Product Family Command Reference*.

Maintenance

With the Fibre Channel gateway expansion module, you can perform the following tasks:

- Add a gateway card to your server switch to expand your current port count.
- Hot-swap expansion modules.
- Replace an older expansion module with a newer, more efficient, and higher-capacity module.

You can add and remove Fibre Channel gateway cards while your server switch runs. You do not disrupt other network configurations when you add and remove cards.

**Caution**

Always ground yourself before you touch any removable cards to avoid damage from electrostatic discharge (ESD).

Software Features

The Fibre Channel gateway module optimizes the performance of the connection between your server switch and your SAN. The features of the gateway can distribute traffic evenly across connections, ensure uninterrupted traffic, and control host/storage access. The sections that follow provide details about the software features of the Fibre Channel gateway.

Redundancy and High Availability

Fibre Channel gateways support high availability (HA) both among cards and within ITLs when you create redundant paths. HA support among Fibre Channel gateways operates automatically. When multiple Fibre Channel gateways in an IB fabric provide the same host access to a storage device, the gateways can evenly distribute the traffic among themselves. When you add another gateway, you can redistribute the traffic so that the new gateway handles a share of the traffic. If one gateway becomes unavailable, the other gateways automatically adopt the traffic of the unavailable gateway.

HA support within ITLs consists of three mutually-exclusive features:

- dynamic gateway port load balancing
- dynamic path affinity
- dynamic gateway port failover

You can configure the feature that you want to run. For more information, see the [“Global Attributes”](#) chapter.

Load Balancing

When both ports of a Fibre Channel gateway provide paths to the same storage, you can configure load balancing to distribute traffic evenly between both ports.

Path Affinity

Path affinity locks a storage connection to a path for the duration of data transfer. Path affinity reduces context switching on the target side to provide greater efficiency for certain types of RAID devices.

Failover

When both ports of a Fibre Channel gateway provide paths to the same storage, you can configure failover so that one port remains dormant while the other port manages all traffic. If the active port fails, the dormant port on the gateway adopts the traffic.

**Note**

Even when you activate dynamic port load balancing or dynamic path affinity on a Fibre Channel gateway, the dynamic port failover feature continues to function.

Access Control

The Fibre Channel gateway supports industry-standard Fibre Channel access controls that use port-based zoning or LUN-based restrictions and permissions. The gateway also provides additional security filters that you can apply individually or collectively to initiators and Fibre Channel storage targets and LUNs.

The Storage Manager on your server switch provides access filters as an additional level of access control. Access filters grant or deny hosts access to ports or to LUNs. See the [“Global Attributes”](#) chapter for more information about how to configure access filters.

Zoning

Zoning grants or denies hosts access to ports on storage targets in the SAN. Soft zones dictate which hosts can access which servers based on WWNNs and WWPNS. You can include in a zone any IB host that connects to the SAN through the Fibre Channel gateway.

LUN Masking

LUN masking grants or denies hosts access to LUNs. LUN masking policies apply to IB hosts that connect to the SAN through the Fibre Channel gateway.

Port Masking

You can configure a Fibre Channel gateway to grant or deny a given initiator access to one or more of the Fibre Channel ports on the gateway. Port masking lets you control the routes that SRP hosts can use to access storage devices on the SAN.

Speed

The maximum aggregate throughput of each Fibre Channel gateway port approaches 200 Mbps in one direction and 400 Mbps bi-directionally. Your server switch aggregates Fibre Channel gateway ports to create a 410 Mbps virtual Fibre Channel pipeline to each connected HCA port. The Fibre Channel gateway itself supports aggregate throughput of 800 Mbps, or 70,000 I/O processes (IOPs) per second.

Topologies

The Fibre Channel gateway simulates the following topologies:

- arbitrated loop (AL)
- fabric-attached arbitrated loop

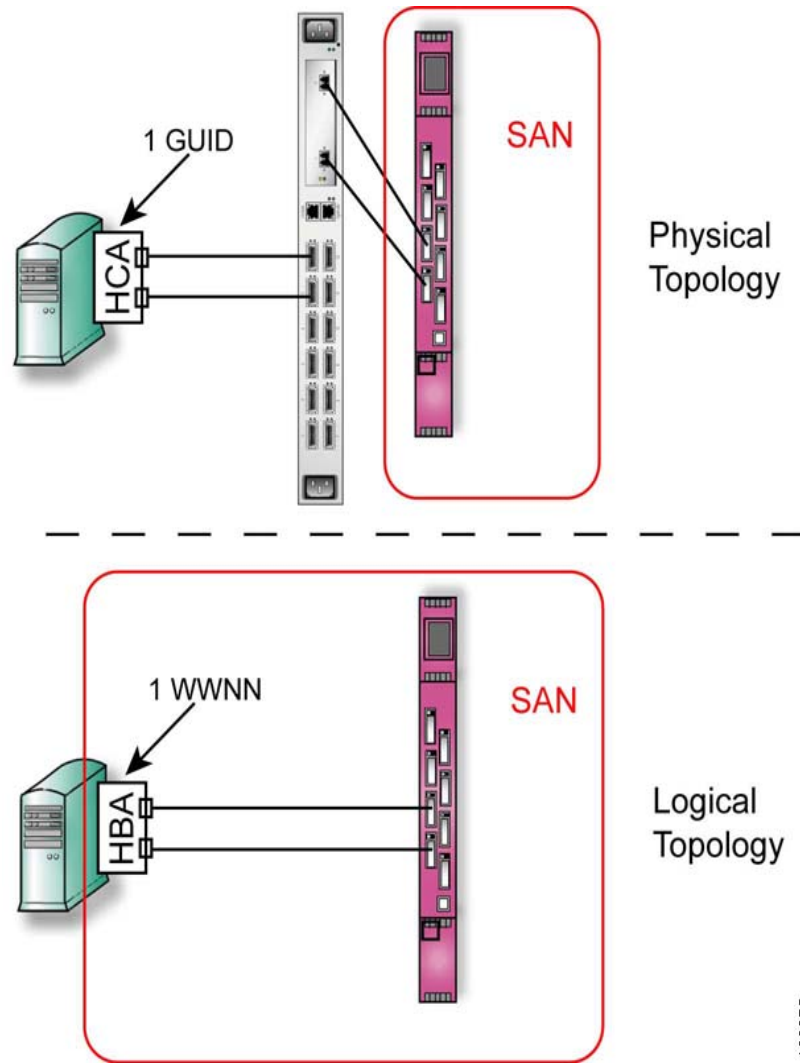
To the SAN, your server switch appears as a hub with Fibre Channel-attached hosts. To the IB fabric, Fibre Channel targets appear as SRP-native storage arrays.

How the Fibre Channel Gateway Works

The Fibre Channel gateway performs transparent topology emulation to connect IB hosts and SANs. The Fibre Channel gateway dynamically allocates world-wide node names (WWNNs) and world-wide port names (WWPNs) to IB hosts to emulate Fibre Channel-attached hosts. The Fibre Channel gateway and IB hosts appear, to the SAN, as groups of hosts on a Fibre Channel hub (see [Figure 1-2](#)) with the dedicated bandwidth advantages of a switch-based architecture. The Fibre Channel gateway translates between the Fibre Channel Protocol (FCP) of the SAN and the SCSI RDMA protocol (SRP) of the IB hosts. In this way, SANs and IB-attached hosts communicate seamlessly. SAN management tools recognize IB and Fibre Channel devices alike in Fibre Channel terms, which permits all management paradigms and security infrastructures to operate normally.

After the Fibre Channel gateway assigns WWNNs and WWPNS to initiators, you must configure access control policies to associate Fibre Channel-attached LUNs to initiators.

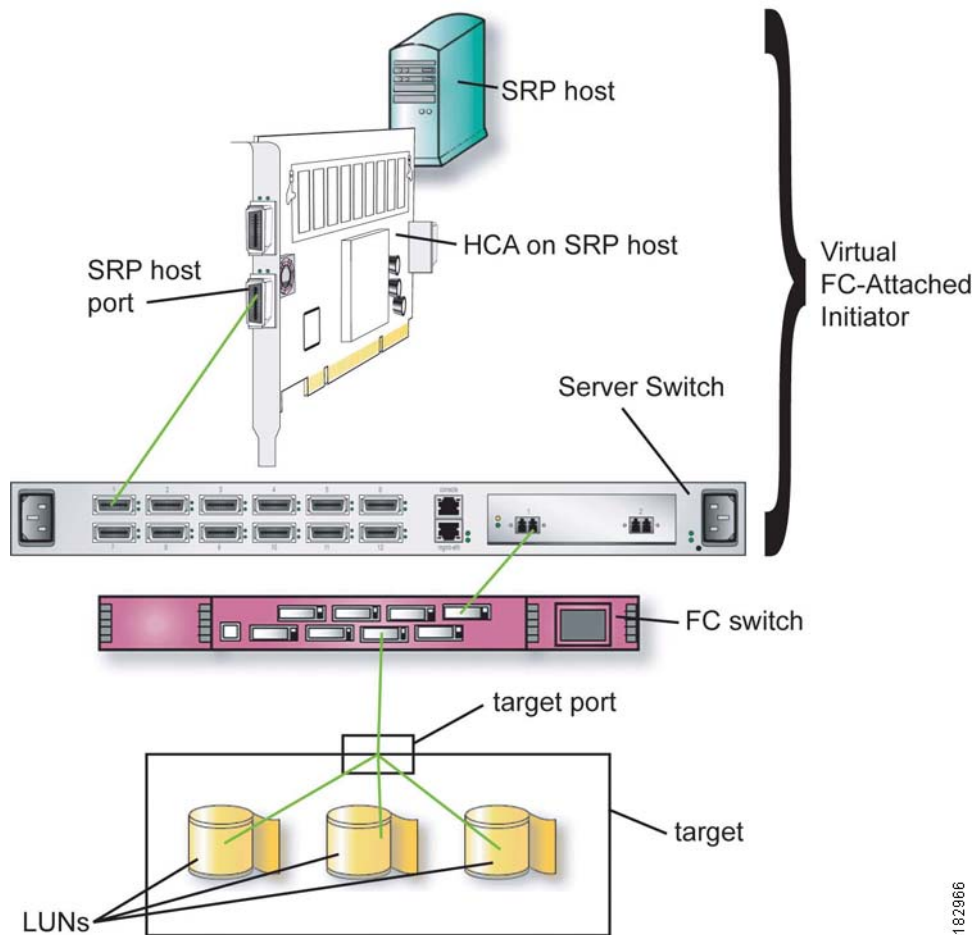
Figure 1-2 Virtualized Fibre Channel Hosts



Initiator-Target-LUN (ITL) Groups

ITLs form the paths between your IB hosts and Fibre Channel storage devices. [Figure 1-3](#) displays the components of an ITL.

Figure 1-3 Components of an ITL



To configure ITLs, see the [“Configuring ITLs” section on page 5-7](#).

Initiators

You configure SRP hosts to serve as initiators. When you configure an ITL, you use the global unique identifier (GUID) of the initiator to specify the host in the ITL. The GUID of an initiator is the GUID of the HCA (not of a port on the HCA). When you configure ITLs, you can grant initiators access to targets and LUNs.

Targets

Fibre Channel storage devices that consist of one or more disks (random devices) or tapes (sequential devices) serve as targets. When you configure an ITL, you use the world-wide port name (WWPN) of a port on the target to specify the target in the ITL.

LUNs

Logical unit numbers (LUNs) represent the individual storage entities in targets. LUNs can represent a disk, a tape, a logical stripe in a RAID array, and so on.



CHAPTER 2

Fibre Channel Gateway High Availability

The following sections appear in this chapter:

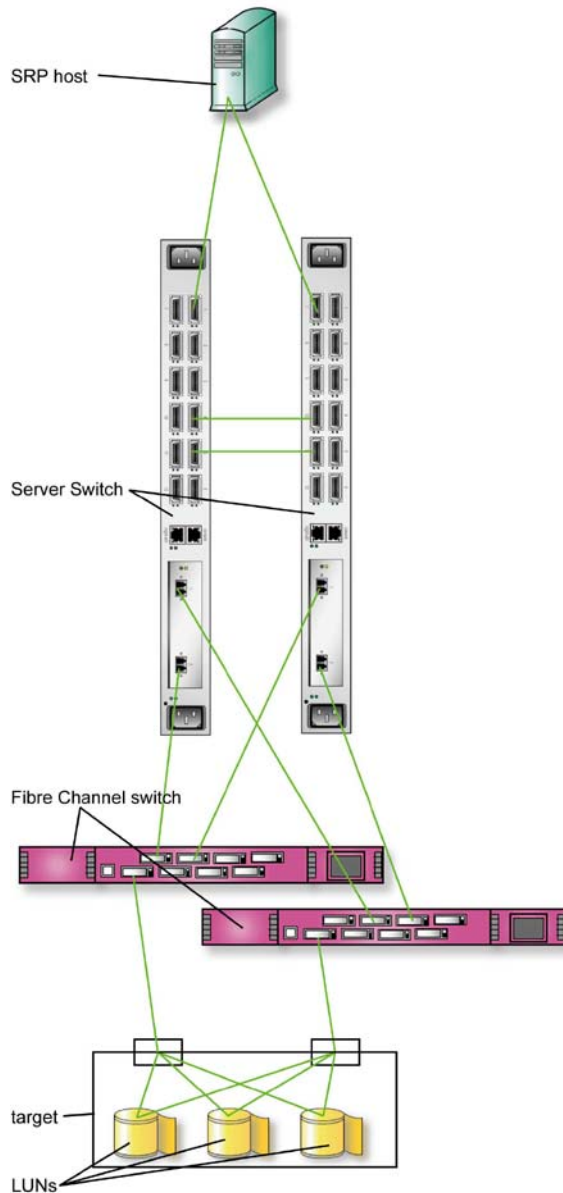
- [Redundant Topologies, page 2-1](#)
- [Dynamic Gateway Failover, page 2-3](#)

Redundant Topologies

High availability (HA) for Fibre Channel gateways depends upon redundant topologies. Observe the following in your redundant topology:

- Every SRP host must be able to reach each storage device through multiple Fibre Channel gateways on the same IB fabric and subnet.
- The two ports of each Fibre Channel gateway must have access to the same storage devices.

[Figure 2-1](#) displays a sample redundant topology.

Figure 2-1 Redundant Topology

In the simple example topology, both Fibre Channel gateways provide the host with a route to the same LUNs, and both of the ports in each Fibre Channel gateway can access the same LUNs. The server switches in the example topology both run on the same IB fabric and in the same subnet (as they directly connect to each other). Because the server switches reside in the same IB fabric and subnet, the device manager monitors the status of both and directs one Fibre Channel gateway to adopt all traffic if the other gateway fails. Because both ports on each gateway access the same LUNs, ITLs over the gateways can support dynamic load balancing, dynamic path affinity, and dynamic port failover.

Load Balancing

The I/Os are load balanced across the ports of a Fibre Channel gateway if the ITL is configured with the load balancing option. The Fibre Channel gateway determines which port the I/O has to transfer by using the load metric that it tracks for each I/O using the size of each I/O.

Dynamic Gateway Failover

Dynamic gateway failover requires no software configuration, only a redundant topology. You can create a redundant topology with multiple server switches, as is, or with one Cisco SFS 3012 that holds multiple Fibre Channel gateways.

When you bring up server switches that meet the topology requirements from the [“Redundant Topologies” section on page 2-1](#), gateway failover occurs automatically. However, when you recover a failed Fibre Channel gateway or add a new Fibre Channel gateway to a production fabric, you must redistribute the traffic.

Recovering from a Fibre Channel Gateway Failure or Disconnect

This section assumes redundant topologies.

Expected Behavior Due to Failover

In the event that a Fibre Channel gateway goes down or is disengaged for any reason, all connections through that link automatically fail over to another Fibre Channel gateway. The failover proceeds as follows:

- The hardware times out on the initiator-target (IT) connection that has been broken.
- A new connection request is sent to the Connection Manager (CM).
- The CM redirects the connection to the new gateway.

Expected Impact to the System

Multiple paths are available between hosts and storage, so if one gateway fails or is removed, traffic and all SRP connections are automatically moved to the other gateway(s).

When a redundantly configured Fibre Channel gateway fails or is disconnected, the following events occur:

- Connections through that gateway are momentarily broken from the host driver’s point of view; the host makes a new connection quickly enough so that an application will not notice the loss of connectivity.
- When the Fibre Channel gateway is replaced or reinserted, the gateway load must be redistributed. See the [“Redistributing Traffic and SRP Connections” section on page 2-4](#) for more information.

Necessary Actions to Recover

If a gateway needs to be replaced for any reason, perform the following steps to reinstate redundancy between Fibre Channel gateways:

-
- Step 1** Install the new Fibre Channel gateway.
 - Step 2** Configure redundant connections from the Fibre Channel gateway to the Fibre Channel storage device.
 - Step 3** Follow the instructions for enabling and configuring a new Fibre Channel gateway.
 - Step 4** Redistribute SRP connections. (See the [“Redistributing Traffic and SRP Connections”](#) section on page 2-4.)

After an absent gateway is reinstalled, the administrator must re-establish the gateway on the system; this step is necessary so that connections are redistributed for load-balancing.

Redistributing Traffic and SRP Connections

In an active fabric, redistribute traffic when you recover a failed Fibre Channel gateway or add a new Fibre Channel gateway that causes the gateway to assume a share of the traffic and connections.

Using Element Manager

To redistribute traffic among multiple Fibre Channel gateways with the Element Manager, perform the following steps:

-
- Step 1** Launch Element Manager and connect to your server switch.
 - Step 2** From the Fibre Channel menu, select **Storage Manager**. The Storage Manager window opens.
 - Step 3** Expand the **Gateway Cards** folder in the Storage navigation tree.
 - Step 4** Click an active gateway. The Redistribute Connections button appears in the right-hand display.
 - Step 5** Click the **Redistribute Connections** button. Any inactive gateways assume a share of the traffic of the gateway that you redistributed.
 - Step 6** Repeat this process for all active gateways.

**Note**

If you need to redistribute the traffic of multiple gateways over one new gateway, you can log the host out of the storage, then log it back in. When it logs in, it will query the device manager and the device manager will alert it to links through the new/fixed gateway.

Using the CLI

To redistribute traffic among multiple Fibre Channel gateways with the CLI, perform the following steps:

- Step 1** Open a CLI session and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super  
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **interface** command with

- the **gateway** keyword
- the slot number of an active gateway

to enter Fibre Channel Interface Configuration submode.

```
SFS-3012R(config)# interface gateway 5  
SFS-3012R(config-if-gw-5/1)#
```

- Step 5** Enter the **no fc srp initiator-target** command to redistribute SRP connections.

```
SFS-3012R(config-if-gw-5/1)# no fc srp initiator-target
```

- Step 6** Repeat this process for all active gateways.



Note If you need to redistribute the traffic of multiple gateways over one new gateway, you can log the host out of the storage, and then log it back in. When it logs in, it will query the device manager, and the device manager will alert it to links through the new/fixed gateway.



CHAPTER 3

Global Attributes

The following sections appear in this chapter:

- [About Global Attributes, page 3-1](#)
- [Configuring Global Attributes, page 3-1](#)
- [Viewing Global Attributes, page 3-10](#)

About Global Attributes

When you configure global attributes, you create a series of default characteristics that automatically apply to all initiators, ITs, and ITLs that you add thereafter. The global attributes that you configure automatically apply to every ITL series that you create after that. Your device only applies global attributes to an ITL when you create the ITL. If you make changes to the global attributes on your device, those changes do not propagate to your existing ITLs; they only apply to new ITLs as you create them.



Note

Configure global attributes before you configure individual initiators, ITs, and ITLs. When you add initiators, ITs, and ITLs, you can customize them on an individual basis. For instance, use global attributes to deny all LUN access to all new initiators, and then grant each initiator access to just the LUNs that you want them to access.

Configuring Global Attributes

Configure global Initiator, IT, and ITL attributes with the CLI or Element Manager.

Using Element Manager

With Element Manager, you can configure all global attributes in one screen. If you opt to use the CLI, (see the [“Using the CLI” section on page 3-4](#)) you must configure each attribute individually.

Configuring All Global Attributes

To configure global attributes with the Element Manager GUI, perform the following steps:

-
- Step 1** Launch Element Manager and connect to your server switch.
- Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.
- Step 3** (Optional) In the Hosts section, check the **Restricted** checkbox in the Gateway Port Access field to deny all new initiators access to all physical Fibre Channel ports on your server switch.



Note If you restrict gateway port access, see the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10 or the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9 to configure ITLs.

- Step 4** (Optional) In the Hosts section, check the **Restricted** checkbox in the LUN Access field to deny all new initiators access to all LUNs on the SAN.



Note If you restrict LUN access, see the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10 or the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9 to configure ITLs.

- Step 5** (Optional) In the Random Access Devices section, enter an integer value from 1 - 256 in the ITL High Mark field to configure the maximum number of requests that the initiator can send per LUN. (Optional) Repeat this process in the Sequential Access Devices section.
- Step 6** (Optional) In the Random Access Devices section, enter an integer value from 1 - 100 in the ITL Max Retries field to limit the maximum number of times that the initiator can send the same I/O to a LUN. (Optional) Repeat this process in the Sequential Access Devices section.
- Step 7** (Optional) In the Random Access Devices section, enter an integer value from 1 - 1800 in the ITL Min IO Timeout field to limit the maximum number of seconds that the initiator can wait for a LUN to accept I/O traffic. Repeat this process in the Sequential Access Devices section.
- Step 8** (Optional) In the Random Access Devices section, click a radio button in the ITL Dynamic Pathing field to configure the dynamic pathing that you want to use. For more information, see these sections:
- [Path Affinity, page 1-5.](#)
 - [Load Balancing, page 1-5.](#)
 - [Failover, page 1-5.](#)
- Repeat this process in the Sequential Access Devices section.
- Step 9** Click the **Apply** button.
-

Granting LUN Access to Initiators through New ITLs

To grant LUN access to initiators, perform the following steps:

-
- Step 1** Launch Element Manager, and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.
 - Step 3** In the Hosts section, uncheck the **Restricted** checkbox in the LUN Access field to grant all initiators access to LUNs through new ITLs.
 - Step 4** Click the **Apply** button.
-

Denying LUN Access to Initiators through New ITLs

To deny LUN access to initiators, perform the following steps:

-
- Step 1** Launch Element Manager and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.
 - Step 3** In the Hosts section, check the **Restricted** checkbox in the LUN Access field to deny all initiators access to LUNs through new ITLs.



Note If you restrict LUN access, see the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10 or the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9 to configure ITLs.

- Step 4** Click the **Apply** button.
-

Granting Port Access to Initiators through New ITLs

To grant port access to initiators, perform the following steps:

-
- Step 1** Launch Element Manager and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.
 - Step 3** In the Hosts section, uncheck the **Restricted** checkbox in the Gateway Port Access field to grant initiators access, through all new ITLs, to physical Fibre Channel ports on your server switch.
 - Step 4** Click the **Apply** button.
-

Denying Port Access to Initiators through New ITLs

To deny port access to initiators, perform the following steps:

-
- Step 1** Launch Element Manager and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.
 - Step 3** In the Hosts section, check the **Restricted** checkbox in the Gateway Port Access field to deny initiators access, through all new ITLs, to physical Fibre Channel ports on your server switch.



Note If you restrict gateway port access, see the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10 or the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9 to configure ITLs.

- Step 4** Click the **Apply** button.
-

Using the CLI

With the CLI, you must configure each global attribute individually. As with the GUI, you must configure some attributes once for random devices and once for sequential devices. The **fc srp-global** command configures random devices by default. Use the **sequential** keyword in each task to configure the attribute for sequential devices.



Note To view current global settings with the CLI, enter the **show fc srp-global** command in User Exec mode or Privileged Exec mode.



Note If you enter a Fibre Channel command and receive an error message that reads, “Operation temporarily failed - try again,” give your Fibre Channel gateway time to finish initializing, then retry the command.

Configuring Global ITL I/O High Mark

To configure the I/O high mark for all new ITLs, perform the following steps:

-
- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

Login: **super**
Password: **xxxxxx**

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

SFS-3012R> **enable**
SFS-3012R#

Step 3 Enter the **configure terminal** command to enter Global Configuration mode.

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

Step 4 Enter the **fc srp-global itl** command and follow it with

- a. (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
- b. the **io-hi-mark** keyword.
- c. an integer value from 1 - 256

to configure the high mark.

```
SFS-3012R(config)# fc srp-global io-hi-mark 5
SFS-3012R(config)#
```

Configuring Global ITL Maximum Retries

To configure the maximum number of retries for all new ITLs, perform the following steps:

Step 1 Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

Step 2 Enter the **enable** command to enter Privileged Exec mode.

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

Step 3 Enter the **configure terminal** command to enter Global Configuration mode.

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

Step 4 Enter the **fc srp-global itl** command and follow it with

- a. (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
- b. the **max-retry** keyword
- c. an integer value from 1 - 100

to configure the max-retry value.

```
SFS-3012R(config)# fc srp-global max-retry 5
SFS-3012R(config)#
```

Configuring Global ITL Minimum I/O Timeout

To configure the minimum I/O timeout for all new ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global itl** command and follow it with

- (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
- the **min-io-timeout** keyword.
- an integer value (seconds) from 1 - 1800

to configure the timeout.

```
SFS-3012R(config)# fc srp-global itl min-io-timeout 200
SFS-3012R(config)#
```

Configuring Global Dynamic Path Affinity

Dynamic path affinity maintains a path for the duration of the data transfer for greater speed and efficiency. To enable dynamic path affinity on all new ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global itl** command and follow it with
- (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
 - the **dynamic-path-affinity** keyword
- to enable dynamic path affinity.



Note This process disables load balancing and failover on new ITLs.

```
SFS-3012R(config)# fc srp-global dynamic-path-affinity
SFS-3012R(config)#
```

Configuring Global Dynamic Gateway Port Load Balancing

Dynamic port load balancing distributes traffic on a gateway evenly between the ports on the gateway when the ports have separate paths to the same storage. To enable dynamic port load balancing on all new ITLs, perform the following steps:

- Step 1** Open a CLI session and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global itl** command and follow it with
- (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
 - the **dynamic-gateway-port-loadbalancing** keyword
- to enable dynamic load balancing.



Note This process disables path affinity and failover on new ITLs.

```
SFS-3012R(config)# fc srp-global dynamic-gateway-port-loadbalancing
SFS-3012R(config)#
```

Configuring Global Dynamic Port Failover

When two ports on a gateway have separate paths to the same storage, you can apply dynamic port failover so that one port remains dormant while the other runs. The dormant port adopts the traffic if the active port fails. To enable dynamic failover on all new ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global itl** command and follow it with

- a. (Optional) the **sequential** keyword (if you want to configure this global attribute for sequential devices)
- b. the **dynamic-gateway-port-failover** keyword

to enable dynamic port failover.



Note This process disables path affinity and load balancing on new ITLs.

```
SFS-3012R(config)# fc srp-global dynamic-gateway-port-failover
SFS-3012R(config)#
```

Granting LUN Access to Initiators through New ITLs

You can only configure global attributes to grant access to all LUNs or deny access to all LUNs. You cannot grant all new initiators access to some LUNs but not others with global policies. To configure LUN access with Element Manager, see the [“Configuring Global Attributes” section on page 3-1](#).

To configure LUN access to new ITs and ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **no fc srp-global lun-policy restricted** command to deny initiators access to all LUNs.

```
SFS-3012R(config)# no fc srp-global lun-policy restricted
SFS-3012R(config)#
```

Denying LUN Access to Initiators through New ITLs

To configure LUN access to new ITs and ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global lun-policy restricted** command to deny initiators access to all LUNs.

```
SFS-3012R(config)# fc srp-global lun-policy restricted
SFS-3012R(config)#
```

Granting Port Access to Initiators through New ITLs

You can only configure global attributes to grant access to all ports or deny access to all ports. You cannot grant all new ITLs access to particular ports. To configure port access with Element Manager, see the [“Configuring Global Attributes” section on page 3-1](#).

To grant port access through new ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **no fc srp-global gateway-portmask-policy restricted** command to grant access to all ports.

```
SFS-3012R(config)# no fc srp-global gateway-portmask-policy restricted
SFS-3012R(config)#
```

Denying Port Access to Initiators through New ITLs

To deny port access through new ITLs, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp-global gateway-portmask-policy restricted** command to grant access to all ports.

```
SFS-3012R(config)# fc srp-global gateway-portmask-policy restricted
SFS-3012R(config)#
```

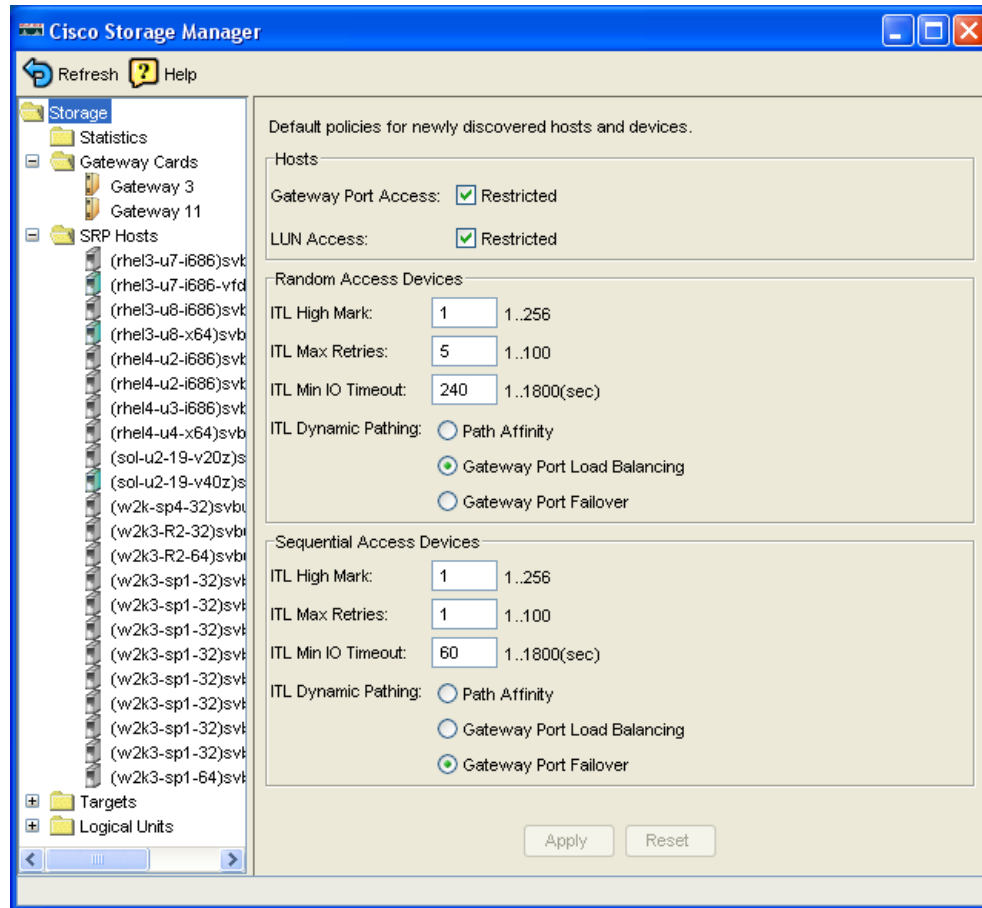
Viewing Global Attributes

View global attributes to determine what policies and configurations immediately apply to new ITLs when you create them. After you understand the global attributes that apply to each ITL, you can customize the attributes of individual ITLs.

Viewing with the Element Manager

- Step 1** Launch Element Manager and connect to your server switch.
- Step 2** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens and displays Default policies for newly discovered hosts and devices. (See [Figure 3-1](#).) If the storage manager is open already, click the **Storage** folder.

Figure 3-1 Element Manager Global Attributes Display



Viewing with the CLI

To view global attributes with the CLI, perform the following steps:

- Step 1** Open a CLI session and log in.

Login: **super**
Password: **xxxxxx**

- Step 2** Enter the **show fc srp-global** command. A list of global attributes appears.

SFS-3012R> **show fc srp-global**

```
=====
                        SRP Global Information
=====
      default-gateway-portmask-policy : non restricted
              default-lun-policy : non restricted
              default-itl-hi-mark : 16
              default-itl-max-retry : 5
              default-itl-min-io-timeout : 10
      default-itl-dynamic-path-affinity : false
default-itl-dynamic-gateway-port-load-balancing : true
      default-itl-dynamic-gateway-port-failover : false
              default-seq-itl-hi-mark : 1
              default-seq-itl-max-retry : 1
              default-seq-itl-min-io-timeout : 60
      default-seq-itl-dynamic-path-affinity : false
default-seq-itl-dynamic-gateway-port-load-balancing : false
      default-seq-itl-dynamic-gateway-port-failover : true
SFS-3012R>
```



CHAPTER 4

Installing and Configuring Hardware

This chapter includes the following sections:

- [Installing a Fibre Channel Gateway, page 4-1](#)
- [Removing a Fibre Channel Gateway, page 4-2](#)
- [Interpreting LEDs, page 4-2](#)

Installing a Fibre Channel Gateway

To install a Fibre Channel gateway expansion module in your server switch, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Properly ground yourself to avoid potential ESD discharge and damage to hardware. |
| Step 2 | Remove the blanking panel from the slot if you have not done so already. |
| Step 3 | Open the ejector lever completely (pull the D-shaped end of the lever down and away from the card). |
| Step 4 | Insert the card into the open slot. |
| Step 5 | Close the ejector lever completely. |
-

For more information, see Step 2 of the “Hardware Installation Steps” section in the *Cisco VFrame Evaluation Test Plan* document.

Connecting to a Fibre Channel SAN

Connect your Fibre Channel gateway to a SAN switch with small form-factor pluggable (SFP) connectors. After you install and connect your gateway, see Chapter 5, [Chapter 5, “Using the Fibre Channel Gateway,”](#) to configure your gateway.



Note

To use redundancy features, when you connect your Fibre Channel gateway to a SAN, connect the gateway ports such that both ports can access the same storage devices. To use ITL features such as dynamic port load balancing (see the [“Configuring Dynamic Load Balancing” section on page 5-37](#)) and dynamic port failover (see the [“Configuring Dynamic Failover” section on page 5-38](#)), both ports on a gateway must be able to access the same storage devices.

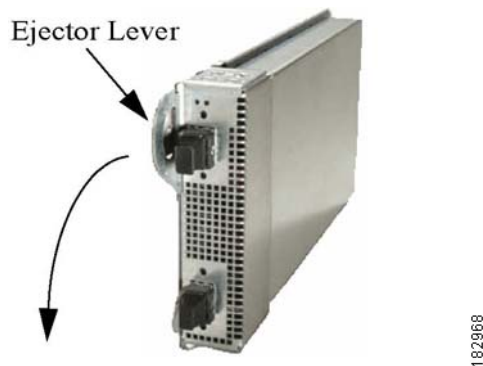
For the VFrame Evaluation Test Plan, continue to Step 1 of the “Hardware Configuration Steps” section in the *Cisco VFrame Evaluation Test Plan* document.

Removing a Fibre Channel Gateway

To remove a Fibre Channel gateway from your server switch, perform the following steps:

-
- Step 1** If possible, take the Fibre Channel gateway offline. Refer to the **shutdown** command in the *Cisco SFS Product Family Command Reference*.
 - Step 2** Properly ground yourself to avoid potential ESD discharge and damage to the card.
 - Step 3** Secure the chassis.
 - Step 4** Open the ejector lever completely: pull the D-shaped end of the lever (see [Figure 4-1](#)) away from the card.

Figure 4-1 Fibre Channel Gateway with Ejector Lever



- Step 5** Pull the lever toward you to remove the card from the chassis.
 - Step 6** Replace the card with another card or a blanking panel.
-

Interpreting LEDs

The following two types of LEDs appear on Fibre Channel interface cards:

- Fibre Channel Interface LEDs (currently inactive)
- Fibre Channel Port LEDs

For this release, Fibre Channel Interface LEDs remain inactive. Fibre Channel Port LEDs indicate port status and activity.

[Figure 4-2](#) shows the Fibre Channel port LEDs.

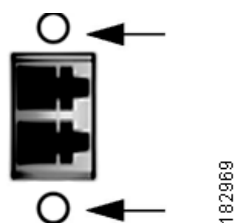
Figure 4-2 Fibre Channel Port LEDs

Table 4-1 lists and interprets Fibre Channel port status LED behavior.

Table 4-1 Fibre Channel Port Status LED Behavior

LED Behavior	Indication
unlit	Port does not detect a connection.
solid green	Port detects a connection but no traffic currently passes through the port.
sporadic flickering green	Port runs successfully and detects traffic.

Table 4-2 lists and interprets Fibre Channel port speed LED behavior.

Table 4-2 Fibre Channel Port Speed LED Behavior

LED Behavior	Indication
unlit	1 Gbps
persistent green	2 Gbps



CHAPTER 5

Using the Fibre Channel Gateway

This chapter includes the following sections:

- [Configuring a Fibre Channel Gateway, page 5-1](#)
- [Administering the Fibre Channel Gateway, page 5-2](#)
- [Configuring Initiators, page 5-5](#)
- [Configuring Targets and LUNs, page 5-6](#)
- [Configuring Initiator-Target Pairs, page 5-6](#)
- [Configuring ITLs, page 5-7](#)
- [Configuring Port Access on Existing ITs and ITLs, page 5-21](#)
- [Viewing Port Access Settings, page 5-25](#)
- [Configuring LUN Access on Existing ITLs, page 5-27](#)
- [Viewing LUN Access Settings, page 5-31](#)
- [Configuring Individual ITL Attributes, page 5-32](#)
- [Gateway Grouping, page 5-40](#)

Configuring a Fibre Channel Gateway

This chapter provides steps to perform Fibre Channel gateway-related tasks. This section provides a high-level view of what tasks to perform when you do the following:

- Install a new gateway
- Update existing configurations

Configuring a New Fibre Channel Gateway

When you first install your Fibre Channel gateway, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Bring up your gateway (see the “Bringing Up a Card” section on page 5-2) so that it can pass traffic. |
| Step 2 | Configure global SRP/ITL attributes (see the “Configuring Global Attributes” section on page 3-1) to assign default attributes to new ITLs. |
| Step 3 | Discover ITLs (see the “Configuring ITLs” section on page 5-7) to provide communication paths between hosts and storage. |
| Step 4 | Customize ITLs and ITs (see the “Configuring Individual ITL Attributes” section on page 5-32) to grant or deny storage access beyond defaults and to configure custom behavior beyond defaults. |
-

Updating Existing Configurations

To make changes to existing Fibre Channel gateway configurations, perform any one of the following tasks:

- Reconfigure global ITL attributes ([“Configuring Global Attributes” section on page 3-1](#)) to change the default configuration of new ITLs.

**Note**

Remember that when you change global defaults, existing ITLs that you created with the original defaults *do not change*. You must reconfigure existing ITLs individually.

-
- Reconfigure existing ITLs (see the [“Configuring Individual ITL Attributes” section on page 5-32](#)) to update access and behavior as your SAN priorities and requirements change.
 - Add additional ITLs (see the [“Configuring ITLs” section on page 5-7](#)) as you add storage devices and hosts.

Administering the Fibre Channel Gateway

Use Element Manager or the CLI to administer your Fibre Channel gateway cards.

Bringing Up a Card

Bring up interface cards to run traffic between IB hosts and Fibre Channel storage.

Using Element Manager

To bring up a Fibre Channel gateway card with Element Manager, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Launch Element Manager, and connect to your server switch. |
| Step 2 | Double-click the card that you want to bring up. The Fibre Channel Card # window opens, where # is the number of the slot that contains the card. |

**Note**

Check the Card Boot Status field to verify that the card has booted successfully. Do not proceed until the Card Boot Status field displays **success** and the Card Boot Stage field displays **done**.

Step 3 Click the **up** radio button in the Enable/Disable Card field.

Step 4 Click the **Apply** button.

Using the CLI

To bring up a Fibre Channel gateway card with the CLI, perform the following steps:

Step 1 Open a CLI session,, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, see the *Cisco SFS Product Family Command Reference*.

Login: **super**
Password: **xxxxxx**

Step 2 Enter the **enable** command to enter Privileged Exec mode.

SFS-3012R> **enable**
SFS-3012R#

Step 3 Enter the **show card** command to verify that your card has booted successfully.

**Note**

Do not proceed until the boot stage field displays “done” and the boot status field displays “success.”

SFS-3012R# show card

```
=====
                        Card Information
=====
      admin      oper      admin  oper  oper
slot type      type      status status code
-----
1   controller  controller  up    up    normal
5   fc2port2G   fc2port2G   down  down  normal
7   fc2port2G   fc2port2G   up    up    normal
16  ib12port4x  ib12port4x  up    up    normal
=====

                        Card Boot Information
=====
      boot      boot      boot
slot stage      status      image
-----
1   done        success      TopspinOS-2.0.0/build447
5   none        none
7   done        success      TopspinOS-2.0.0/build447
16  done        success      TopspinOS-2.0.0/build447
=====

                        Card Seeprom
=====
      product      pca      pca      fru
slot serial-number serial-number number  number
=====
```

```

-----
1    PY-0305-000017    PY-0305-000017    95-00005-01-B3    98-00001-01
5    PY-0309-000023    PY-0309-000023    95-00008-01-C1    0
7    PY-0244-000007    PY-0244-000007    95-00008-01-B0    0
16   PY-0307-000028    PY-0307-000028    95-00006-01-B1    0

```

Step 4 Enter the **configure terminal** command to enter Global Configuration mode.

```

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

```

Step 5 Enter the **card** command and the slot number in which your Fibre Channel gateway resides.

```

SFS-3012R(config)# card 5
SFS-3012R(config-card-5)#

```

Step 6 Enter the **no shutdown** command to bring up the card.

```

SFS-3012R(config-card-5)# no shutdown
SFS-3012R(config-card-5)#

```

Bringing Down a Card

To bring down a card with Element Manager, perform the steps documented above, but click the **down** radio button in Step 3.

To bring down a card with the CLI, perform the steps documented above, but use the **shutdown** command in Step 6.

Bringing Up a Port

Bring up interface ports to run traffic over the port.

Using Element Manager

To bring up a Fibre Channel gateway port with Element Manager, perform the following steps:

-
- Step 1** Launch Element Manager, and connect to your server switch.
 - Step 2** Double-click the port that you want to bring up. The Fibre Channel Port card#/port# window opens, where *slot#* is the slot of the Fibre Channel gateway card and *port#* is the port number on the card.
 - Step 3** Click the **up** radio button in the Enable/Disable Port field.
 - Step 4** Click the **Apply** button.
-

Using the CLI

To bring up a Fibre Channel gateway card with the CLI, perform the following steps:

- Step 1** Open a CLI session,, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **interface** command with

- the **fc** keyword
- the slot#/port# identifier of the port

to enter Fibre Channel Interface Configuration submode.

```
SFS-3012R(config)# interface fc 5/1
SFS-3012R(config-if-fc-5/1)#
```

- Step 5** Enter the **no shutdown** command to bring up the card.

```
SFS-3012R(config-if-fc-5/1)# no shutdown
SFS-3012R(config-if-fc-5/1)#
```

Bringing Down a Port

To bring down a port with Element Manager, perform the steps documented above, but click the **down** radio button in Step 3.

To bring down a port with the CLI, perform the steps documented above, but use the **shutdown** command in Step 5.

Configuring Initiators

When you configure initiators, you assign Fibre Channel WWNNs to SRP hosts so the SAN can recognize the hosts. For information about how to configure initiators, see the [“Configuring ITLs” section on page 5-7](#).



Note

You can configure initiators that you have not yet connected to your fabric. You can enter the GUID of the initiator into the CLI or Element Manager so the configuration works when you connect the SRP host.

Configuring Targets and LUNs

The Fibre Channel gateway automatically detects and configures the storage that it discovers. For information about how to configure targets and LUNs, see the “[Configuring ITLs](#)” section on page 5-7. To configure targets and LUNs manually, refer to the **fc srp target** and **fc srp lu** commands in the *Cisco SFS Product Family Command Reference*.

Configuring Initiator-Target Pairs

You can manually configure Initiator-Target pairs (ITs) independently of LUNs/LUs. In particular, you can configure ITs to form a staging area before your storage over IB goes into production. For more information, refer to the **fc srp it** command in the *Cisco SFS Product Family Command Reference*.

Configuring IT Pair Mode for Persistent Binding

When you configure a VFrame system (for details, refer to the *Cisco VFrame InfiniBand Director User Guide* and *Cisco VFrame InfiniBand Third-Party Integration Guide*), you can place your IT pairs in test mode to test persistent connections before you bring up your SRP hosts.

Configuring Test Mode with the CLI

To configure test mode with the CLI, perform the following steps:

-
- Step 1** Log in to your server switch.
- Enter the **enable** command to enter Privileged Execute mode.
- ```
SFS> enable
SFS#
```
- Step 2** Enter the **configure terminal** command to enter Global Configuration mode.
- ```
SFS# configure terminal
SFS(config)#
```
- Step 3** Enter the **fc srp it** command with the following:
- the GUID of the initiator
 - the GUID extension of the initiator
 - the WWPN of the target
 - the test-mode keyword
- to configure the IT pair to test mode.
- ```
SFS(config)# fc srp it 00:05:ad:00:00:00:16:ff 00:00:00:00:00:00:00:00
21:00:00:04:cf:86:a0:1f test-mode
```
-

## Configuring Test Mode with Element Manager

To configure test mode with Element Manager, perform the following steps:

- Step 1** Click the **FibreChannel** menu and select **Storage Manager**. The Storage Manager window opens.
- Step 2** Click the plus-sign (+) next to the SRP Hosts folder to expand the folder. A list of configured initiators appears beneath the SRP Hosts folder.
- Step 3** Click the initiator whose connections to targets you want to view, and then click the **Targets** tab. The Targets visible to this host table appears in the right-hand display.
- Step 4** Click the entry of the IT pair that you want to configure, and then click the **Edit** button. An IT Properties window opens.
- Step 5** In the Mode field, click the **Normal** radio button or the **Test** radio button.



### Note

The Current Access field must not contain any entries in order for you to configure the mode.

## Configuring ITLs

You must configure ITLs for your initiators to communicate with your storage. You can configure ITLs with the CLI or the Element Manager graphical user interface (GUI).

- If you restricted port and LUN access when you configured global attributes, proceed to the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9 or the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10.
- If you did not configure access, perform the steps below.



### Note

If you enter a Fibre Channel command and receive an error message that reads, “Operation temporarily failed - try again,” give your Fibre Channel gateway time to finish initializing, and then retry the command.

## Configuring ITLs with Element Manager while No Global Policy Restrictions Apply

Before you configure ITLs, you must log your SRP hosts out of any storage, and then log them back in at the end of the process. The steps below provide a complete example for a Linux host.

Adjust Step 1 and Step 2 appropriately for your host type.

To configure ITLs with a Linux SRP host while your port masking and LUN masking policies are unrestricted, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Enter the `/usr/local/topspin/bin/vstat --verbose|grep -i guid` command to display the host GUID.



**Note** Record the GUID value. You will enter it repeatedly.

- Step 3** Bring up the Fibre Channel gateways on your server switch with the following steps:
- Launch Element Manager.
  - Double-click the Fibre Channel gateway card that you want to bring up. The Fibre Channel Card window opens.
  - Click the **up** radio button in the Enable/Disable Card field, and then click the **Apply** button.
  - (Optional) Repeat this process for additional gateways.

The Fibre Channel gateway automatically discovers all attached storage.



**Note** Discovered LUs remain gray (inactive) until a SRP host connects to them. Once a host connects to a LU, its icon becomes blue (active).

- Step 4** From the FibreChannel menu of the Element Manager, select **Storage Manager**. The Topspin Storage Manager window opens.
- Step 5** Click the **SRP Hosts** folder in the Storage navigation tree in the left-hand frame of the interface. The SRP Hosts display appears in the right-hand frame of the interface.
- Step 6** Click the **Define New** button in the SRP Hosts display. The Define New SRP Host window opens.



**Note** If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

- Step 7** Select a GUID from the Host GUID pulldown menu in the Define New SRP Host window. The menu displays the GUIDs of all connected hosts that you have not yet configured as initiators.
- Step 8** (Optional) Type a description in the Description field in the Define New SRP Host window.
- Step 9** Click the **Next >** button. The Define New SRP Host window displays a recommended WWNN for the host and recommended WWPNNs that will represent the host on all existing and potential Fibre Channel gateway ports.



**Note** You can manually configure the WWNN or WWPNNs, but we *strongly recommend* that you use the default values to avoid conflicts.

- Step 10** Click the **Finish** button. The new host appears in the SRP Hosts display.
- Step 11** Expand the **SRP Hosts** folder in the Storage navigation tree, then click the host that you created. The host display appears in the right-hand frame of the interface.
- Step 12** (Optional) Click the **LUN Access** tab in the host display, then click the **Discover LUNs** button. The targets and associated LUNs that your Fibre Channel gateway sees appear in the Accessible LUNs field.
- Step 13** Click the **Refresh** button in the Topspin Storage Manager window.

## Configuring ITLs with Element Manager while Global Policy Restrictions Apply

Before you configure ITLs, you must log your SRP hosts out of any storage, then log them back in at the end of the process. The steps below provide a complete example for a Linux host. Adjust Step 1 and Step 2 appropriately for your host type.

These instructions apply to environments where the portmask policy and LUN masking policy are both restricted. To verify that you have restricted your policies, enter the **show fc srp-global** command at the CLI. View the **default-gateway-portmask-policy** and **default-lun-policy** fields. If restrictions apply to either field, **restricted** appears in the field output.

To configure ITLs with a Linux SRP host while your port masking and LUN masking policies are restricted, perform the following steps:

- 
- Step 1** Log in to your host.
- Step 2** Enter the **/usr/local/topspin/bin/vstat --verbose|grep -i guid** command at the host CLI to display the host GUID.




---

**Note** Record the GUID value. You will enter it repeatedly.

---

- Step 3** Bring up the Fibre Channel gateways on your server switch with the following steps:
- Launch Element Manager.
  - Double-click the Fibre Channel gateway card that you want to bring up. The Fibre Channel Card window opens.
  - Click the **up** radio button in the Enable/Disable Card field, then click the **Apply** button.
  - (Optional) Repeat this process for additional gateways.

The Fibre Channel gateway automatically discovers all attached storage.




---

**Note** Discovered LUs remain gray (inactive) until an SRP host connects to them. Once a host connects to a LU, its icon becomes blue (active).

---

- Step 4** From the FibreChannel menu, select **Storage Manager...**
- Step 5** Click the **SRP Hosts** folder in the Storage navigation tree in the left-hand frame of the interface. The SRP Hosts display appears in the right-hand frame of the interface.
- Step 6** Click the **Define New** button in the SRP Hosts display. The Define New SRP Host window opens.




---

**Note** If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

---

- Step 7** Select a GUID from the Host GUID pulldown menu in the Define New SRP Host window. The menu displays the GUIDs of all available hosts that you have not yet configured as initiators.
- Step 8** (Optional) Type a description in the Description field in the Define New SRP Host window. If you do not enter a description, your device will assign a description.

- Step 9** Click the **Next >** button. The Define New SRP Host window displays a recommended WWNN for the host and recommended WWPNNs that will represent the host on all existing and potential Fibre Channel gateway ports.



**Note** You can manually configure the WWNN or WWPNNs, but we *strongly recommend* that you use the default values to avoid conflicts.

- Step 10** Click the **Finish** button. The new host appears in the SRP Hosts display.
- Step 11** Expand the **SRP Hosts** folder in the Storage navigation tree, then click the host that you created. The host display appears in the right-hand frame of the interface.
- Step 12** Click the **Targets** tab in the host display. Double-click the WWPNN of the target that you want your host to access. The IT Properties window opens.
- Step 13** Click the button with three dots “...” next to the Port Mask field. The Select Port(s) window opens and displays two port numbers for each slot in the chassis. “Raised” port numbers represent restricted ports. “Pressed” port numbers represent accessible ports.
- Step 14** Click the port(s) to which the SAN connects to “press” them and grant the initiator access to the target through those ports, then click the **OK** button.
- Step 15** Click the **Apply** button in the IT Properties window, then close the window.
- Step 16** Click the **LUN Access** tab in the host display, then click the **Discover LUNs** button. The targets and associated LUNs that your Fibre Channel gateway sees appear in the Available LUNs field.
- Step 17** Click the **LUN Access** tab, click the target that you configured in Step 12, and then click the **Add >** button. The target and its LUN(s) appear in the Accessible LUNs field in an Inactive ITLs folder.
- Step 18** Click the LUN that you want your host to reach, then click the **Edit ITL Properties** button. The ITL Properties window opens.
- Step 19** Click the button with three dots “...” next to the Port Mask field. The Select Port(s) window opens and displays two port numbers for each slot in the chassis. “Raised” port numbers represent restricted ports. “Pressed” port numbers represent accessible ports.
- Step 20** Click the port(s) to which the SAN connects to “press” them and grant the initiator access to the target via those ports, then click the **OK** button.
- Step 21** Click the **Refresh** button in the Topspin Storage Manager window.

## Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1

To configure ITLs without the Element Manager GUI, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Enter the `/usr/local/topspin/bin/vstat --verbose|grep -i guid` command at the host CLI to display the host GUID.



**Note** Record the GUID value. You will enter it repeatedly.

- Step 3** Enter the **no shutdown** command on your server switch CLI to bring up any Fibre Channel gateway cards that connect your device to Fibre Channel storage. The gateway automatically discovers all storage.

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```

- Step 4** (Optional) Enter the **show fc srp target** command to view the storage that your gateway(s) discovered.

```
SFS-3012R# show fc srp target

=====
 SRP Targets
=====
 wwpn: 21:00:00:04:cf:f6:c2:ab
 wwnn: 20:00:00:04:cf:f6:c2:ab
 description: SRP.T10:21000004CFF6C2AB
 ioc-guid: 00:05:ad:00:00:00:15:1a
 service-name: SRP.T10:21000004CFF6C2AB
 protocol-ids: 04:00:00:00:00:00:00:00:00:00
 fc-address: 00:00:ef
 mtu: 0
 connection-type: nl-port
 physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

- Step 5** Enter the **fc srp initiator** command with

- the GUID of the host (from <Link>step 2)
- the GUID extension (always **00:00:00:00:00:00:00:00**)
- the **auto-bind** keyword

to configure your host.



**Note** For an initiator to successfully connect to storage, each physical Fibre Channel gateway port requires a virtual port with a unique WWPN that points to the initiator. Also, the initiator requires a unique WWNN. You can configure these values manually, but we *strongly recommend* that you take advantage of CLI options to assign these values dynamically. The remainder of this process dynamically allocates WWNNs and WWPNS.

The **auto-bind** keyword accomplishes the following:

- assigns a unique WWNN to the initiator
- creates a virtual port (that maps to the initiator) for each possible (actual and potential) physical Fibre Channel gateway ports and assigns a WWPN to each virtual port.

```
SFS-3012R# configure terminal
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:5c 00:00:00:00:00:00:00:00
auto-bind
```



**Note** If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

**Step 6** (Optional) Enter the **fc srp initiator** command with

- the GUID of the host
- the GUID extension
- the **description** keyword

to assign an easily-recognizable identifier to the initiator.

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
description Bender
```

**Step 7** (Optional) Enter the **show fc srp initiator** command to verify the new initiator.

```
SFS-3012R# show fc srp initiator

=====
SRP Initiators
=====
guid: 00:05:ad:00:00:01:29:c5
extension: 00:00:00:00:00:00:00:00
description: Bender
wwnn: 20:01:00:05:ad:00:40:00
credit: 0
active-ports: none
pkeys:
action: auto-bind
result: success
wwpns: port wwpn fc-addr
 2/1 20:01:00:05:ad:20:40:00 00:00:00
 2/2 20:01:00:05:ad:24:40:00 00:00:00
 3/1 20:01:00:05:ad:30:40:00 00:00:00
 3/2 20:01:00:05:ad:34:40:00 00:00:00
 4/1 20:01:00:05:ad:40:40:00 00:00:00
 4/2 20:01:00:05:ad:44:40:00 00:00:00
 5/1 20:01:00:05:ad:50:40:00 00:00:00
 5/2 20:01:00:05:ad:54:40:00 00:00:00
 6/1 20:01:00:05:ad:60:40:00 00:00:02
 6/2 20:01:00:05:ad:64:40:00 00:00:00
 7/1 20:01:00:05:ad:70:40:00 00:00:00
 7/2 20:01:00:05:ad:74:40:00 00:00:00
 8/1 20:01:00:05:ad:80:40:00 00:00:00
 8/2 20:01:00:05:ad:84:40:00 00:00:00
 9/1 20:01:00:05:ad:90:40:00 00:00:00
 9/2 20:01:00:05:ad:94:40:00 00:00:00
 10/1 20:01:00:05:ad:a0:40:00 00:00:00
 10/2 20:01:00:05:ad:a4:40:00 00:00:00
 11/1 20:01:00:05:ad:b0:40:00 00:00:00
 11/2 20:01:00:05:ad:b4:40:00 00:00:00
 12/1 20:01:00:05:ad:c0:40:00 00:00:00
 12/2 20:01:00:05:ad:c4:40:00 00:00:00
 13/1 20:01:00:05:ad:d0:40:00 00:00:00
 13/2 20:01:00:05:ad:d4:40:00 00:00:00
 14/1 20:01:00:05:ad:e0:40:00 00:00:00
 14/2 20:01:00:05:ad:e4:40:00 00:00:00

Total: 1 initiators.

SFS-3012R#
```

**Step 8** Enter the **fc srp initiator** command with

- the GUID of the host
- the GUID extension of the host
- the **discover-itl** keyword

to prompt your device to discover the potential ITLs that your initiator can form.



**Note** This command may take some time to execute.

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
discover-itl
```

**Step 9** Enter the **show fc srp itl** command to display the potential ITLs and record the *target-wwpn* and *fc-lunid* values.

```
SFS-3012R(config)# exit
SFS-3012R# show fc srp itl
```

```
=====
 SRP ITL
=====
 guid: 00:05:ad:00:00:01:29:c5
 extension: 00:00:00:00:00:00:00:00
 target-wwpn: 21:00:00:04:cf:f6:c2:ab
 fc-lunid: 00:00:00:00:00:00:00:00
 srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
 description: itl
 device-category: random
 lun-policy: restricted
non-restricted-ports: none
 active-ports: none
physical-access: 6/1
 hi-mark: 16
 max-retry: 5
 min-io-timeout: 10
dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
 active-slots: none

Total: 1 itls.

SFS-3012R#
```



**Note** The *fc-lunid* field displays the LUN ID of the ITL that you will configure.

**Step 10** Enter the **no fc srp itl** command with

- the GUID of the host
- the GUID extension of the host

- the WWPN of the target (from Step 9)
- the LUN ID of the storage disk (from Step 9)
- the **lun-policy** keyword
- the **restricted** keyword

to configure the ITL through LUN masking.

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted
```

**Step 11** Enter the **no fc srp it** command with

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target
- the **gateway-portmask-policy** keyword
- the **restricted** keyword
- the **all** keyword or the ports you want to unmask

to grant the initiator portmask-policy access to the target.

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

**Step 12** Enter the **no fc srp itl** command with

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target
- the LUN ID of the storage disk
- the **gateway-portmask-policy** keyword
- the **restricted** keyword
- the **all** keyword or the ports you want to unmask

to grant the initiator portmask-policy access to the LUN.

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

**Step 13** Return to User Exec mode or Privileged Exec mode and enter the **show fc srp itl** command to verify that the ITL is active. Port numbers appear in the physical-access and active-ports fields to indicate that the ITL is active.

## Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 2

To configure ITLs without the Element Manager GUI, perform the following steps:

**Step 1** Log in to your host.

**Step 2** Enter the `/usr/local/topspin/bin/vstat --verbose|grep -i guid` command at the host CLI to display the host GUID.



**Note** Record the GUID value. You will enter it repeatedly.

**Step 3** Enter the **no shutdown** command on your server switch CLI to bring up any Fibre Channel gateway cards that connect your device to Fibre Channel storage. The gateway automatically discovers all storage.

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```

**Step 4** (Optional) Enter the **show fc srp target** command to view the storage that your gateway(s) discovered.

```
SFS-3012R# show fc srp target
```

```
=====
 SRP Targets
=====
 wwpn: 21:00:00:04:cf:f6:c2:ab
 wwnn: 20:00:00:04:cf:f6:c2:ab
 description: SRP.T10:21000004CFF6C2AB
 ioc-guid: 00:05:ad:00:00:00:15:1a
 service-name: SRP.T10:21000004CFF6C2AB
 protocol-ids: 04:00:00:00:00:00:00:00:00
 fc-address: 00:00:ef
 mtu: 0
 connection-type: nl-port
 physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

**Step 5** Enter the **fc srp initiator** command with

- the GUID of the host (from Step 2)
- the GUID extension (always **00:00:00:00:00:00:00:00**)
- the **auto-bind** keyword

to configure your host.



**Note** For an initiator to successfully connect to storage, each physical Fibre Channel gateway port requires a virtual port with a unique WWPN that points to the initiator. Also, the initiator requires a unique WWNN. You can configure these values manually, but we *strongly recommend* that you take advantage of CLI options to assign these values dynamically. The remainder of this process dynamically allocates WWNNs and WWPNS.

The **auto-bind** keyword accomplishes the following:

- assigns a unique WWNN to the initiator
- creates a virtual port (that maps to the initiator) for each possible (actual and potential) physical Fibre Channel gateway port and assigns a WWPN to each virtual port.

```
SFS-3012R# configure terminal
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:5c 00:00:00:00:00:00:00:00
auto-bind
```



**Note**

If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

**Step 6** (Optional) Enter the **fc srp initiator** command with

- the GUID of the host
- the GUID extension
- the **description** keyword

to assign an easily-recognizable identifier to the initiator.

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
description Bender
```

**Step 7** (Optional) Enter the **show fc srp initiator** command to verify the new initiator.

```
SFS-3012R# show fc srp initiator
```

```
=====
 SRP Initiators
=====
 guid: 00:05:ad:00:00:01:29:c5
 extension: 00:00:00:00:00:00:00:00
 description: Bender
 wwnn: 20:01:00:05:ad:00:40:00
 credit: 0
 active-ports: none
 pkeys:
 action: auto-bind
 result: success
 wwpns: port wwpn fc-addr
 2/1 20:01:00:05:ad:20:40:00 00:00:00
 2/2 20:01:00:05:ad:24:40:00 00:00:00
 3/1 20:01:00:05:ad:30:40:00 00:00:00
 3/2 20:01:00:05:ad:34:40:00 00:00:00
 4/1 20:01:00:05:ad:40:40:00 00:00:00
 4/2 20:01:00:05:ad:44:40:00 00:00:00
 5/1 20:01:00:05:ad:50:40:00 00:00:00
 5/2 20:01:00:05:ad:54:40:00 00:00:00
 6/1 20:01:00:05:ad:60:40:00 00:00:02
 6/2 20:01:00:05:ad:64:40:00 00:00:00
 7/1 20:01:00:05:ad:70:40:00 00:00:00
 7/2 20:01:00:05:ad:74:40:00 00:00:00
 8/1 20:01:00:05:ad:80:40:00 00:00:00
 8/2 20:01:00:05:ad:84:40:00 00:00:00
 9/1 20:01:00:05:ad:90:40:00 00:00:00
 9/2 20:01:00:05:ad:94:40:00 00:00:00
 10/1 20:01:00:05:ad:a0:40:00 00:00:00
 10/2 20:01:00:05:ad:a4:40:00 00:00:00
```

```

11/1 20:01:00:05:ad:b0:40:00 00:00:00
11/2 20:01:00:05:ad:b4:40:00 00:00:00
12/1 20:01:00:05:ad:c0:40:00 00:00:00
12/2 20:01:00:05:ad:c4:40:00 00:00:00
13/1 20:01:00:05:ad:d0:40:00 00:00:00
13/2 20:01:00:05:ad:d4:40:00 00:00:00
14/1 20:01:00:05:ad:e0:40:00 00:00:00
14/2 20:01:00:05:ad:e4:40:00 00:00:00

Total: 1 initiators.

SFS-3012R#

```

**Step 8** Enter the **no fc srp it** command with

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target
- the **gateway-portmask-policy** keyword
- the **restricted** keyword
- the **all** keyword or the ports you want to unmask

to grant the initiator portmask-policy access to the target.



**Note** The ITLs that you discover in Step 9, below, inherit the attributes of the ITs.

```

SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all

```

**Step 9** Enter the **fc srp initiator** command with

- the GUID of the host
- the GUID extension of the host
- the **discover-itl** keyword

to prompt your device to discover the potential ITLs that your initiator can form.



**Note** This command may take some time to execute.

```

SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00
discover-itl

```

**Step 10** Enter the **show fc srp itl** command to display the potential ITLs and record the *target-wwpn* and *fc-lunid* values.

```

SFS-3012R(config)# exit
SFS-3012R# show fc srp itl

```

```

=====
 SRP ITL
=====
 guid: 00:05:ad:00:00:01:29:c5
 extension: 00:00:00:00:00:00:00:00
 target-wwpn: 21:00:00:04:cf:f6:c2:ab
 fc-lunid: 00:00:00:00:00:00:00:00
 srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
 : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
 description: itl
 device-category: random
 lun-policy: restricted
non-restricted-ports: none
 active-ports: none
 physical-access: 6/1
 hi-mark: 16
 max-retry: 5
 min-io-timeout: 10
 dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
 active-slots: none

```

Total: 1 itls.

SFS-3012R#



**Note**

The `fc-lunid` field displays the LUN ID of the ITL that you will configure. For non-sequential LUNs, this value will always appear as `00:00:00:00:00:00:00:00`. For sequential LUNs, the value will iterate by 1 for each LUN in the target device.

**Step 11** Enter the **no fc srp itl** command with

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target (from Step 9)
- the LUN ID of the storage disk (from Step 9)
- the **lun-policy** keyword
- the **restricted** keyword

to configure the ITL through LUN masking.

```

SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted

```

**Step 12** Return to User Exec mode or Privileged Exec mode and enter the **show fc srp itl** command to verify that the ITL is active. Port numbers appear in the `physical-access` and `active-ports` fields to indicate that the ITL is active.

## Configuring ITLs with Custom WWNNs and WWPNS

If you use a specific WWNN and WWPNS strategy in your SAN and you want devices on the IB fabric to match this strategy, you can manually configure WWNNs and WWPNS for initiators on your IB fabric.



**Note** We strongly recommend that, instead, you auto-bind initiators when you create them.

### Using Element Manager

To use the Element Manager to configure ITLs with custom WWNNs and WWPNS, perform the following steps:

- 
- Step 1** Log in to your host.
- Step 2** Bring up the Fibre Channel gateways on your server switch with the following steps:
- Launch Element Manager.
  - Double-click the Fibre Channel gateway card that you want to bring up. The Fibre Channel Card window opens.
  - Click the **up** radio button in the **Enable/Disable Card** field, then click the **Apply** button.
  - (Optional) Repeat this process for additional gateways.

The Fibre Channel gateway automatically discovers all attached storage.



**Note** Discovered LUs remain gray (inactive) until an SRP host connects to them. Once a host connects to an LU, its icon becomes blue (active).

- Step 3** From the FibreChannel menu, select **Storage Manager**. The Topspin Storage Manager window opens.
- Step 4** Click the **SRP Hosts** folder. The SRP Hosts display appears in the window.
- Step 5** Click the **Define New** button. The Define New SRP Host window opens.



**Note** If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

- Step 6** Select the GUID of the host from the Host GUID pulldown menu or enter the GUID of the host in that field.
- Step 7** (Optional) Enter a description for the initiator in the Description field.
- Step 8** Click the **Next >** button. The Define New SRP Host window displays a suggested WWNN and suggested WWPNS.
- Step 9** Replace the dynamically-generated WWNN in the Host WWNN field with a custom WWNN.



**Caution** Verify that no other device uses this WWNN.

- Step 10** (Optional) Manually alter any WWPNS that you want to customize.

- Step 11** Click the **Finish** button.
- Step 12** To finish the process, see the [“Configuring ITLs with Element Manager while No Global Policy Restrictions Apply”](#) section on page 5-7 or the [“Configuring ITLs with Element Manager while Global Policy Restrictions Apply”](#) section on page 5-9.

## Using the CLI

To use the CLI to configure ITLs with custom WWNNs and WWPNs, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Enter the `/usr/local/topspin/bin/vstat --verbose|grep -i guid` command at the host CLI to display the host GUID.



**Note** Record the GUID value. You will enter it repeatedly.

- Step 3** Enter the **no shutdown** command on your server switch CLI to bring up any Fibre Channel gateway cards that connect your device to Fibre Channel storage. The gateway automatically discovers all storage.
- Step 4** (Optional) Enter the **show fc srp target** command to view the storage that your gateway(s) discovered.

```
SFS-3012R# configure terminal
SFS-3012R(config)# card 6
SFS-3012R(config-card-6)# no shutdown
```

```
SFS-3012R# show fc srp target
```

```
=====
 SRP Targets
=====
 wwpn: 21:00:00:04:cf:f6:c2:ab
 wwnn: 20:00:00:04:cf:f6:c2:ab
 description: SRP.T10:21000004CFF6C2AB
 ioc-guid: 00:05:ad:00:00:00:15:1a
 service-name: SRP.T10:21000004CFF6C2AB
 protocol-ids: 04:00:00:00:00:00:00:00:00
 fc-address: 00:00:ef
 mtu: 0
 connection-type: nl-port
 physical-access: 6/1
Total: 1 targets.

SFS-3012R#
```

- Step 5** Enter the **fc srp initiator** command with
- the GUID of the host (from <Link>step 2)
  - the GUID extension (always **00:00:00:00:00:00:00:00**)
  - the **wwnn** keyword.
  - the WWNN that you want to assign to the initiator
- to configure your host.

**Step 6** Enter the **fc srp initiator-wwpn** command with

- the GUID of the host (from <Link>step 2)
- the GUID extension (always **00:00:00:00:00:00:00:00**)
- the physical Fibre Channel gateway port to which you want to add the WWPN (in slot#/port# format)
- the WWPN that you want to add to the port

to apply a WWPN to the physical Fibre Channel gateway port that delivers Fibre Channel traffic to the SRP host.

**Step 7** To finish the process, see the [“Configuring ITLs with the CLI while Global Restriction Policies Apply, Option 1”](#) section on page 5-10.

## Configuring Port Access on Existing ITs and ITLs

You must configure port access on both ITs and ITLs to successfully pass traffic between an initiator and a LUN.



### Note

When you configure port access on an IT, that access configuration *does not propagate* to the associated ITLs.

## Granting Port Access with Element Manager

To grant an initiator access to a target and LUN through a Fibre Channel gateway port, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Launch Element Manager, and connect to your server switch.
- Step 3** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
- Step 4** Expand the **SRP Hosts** folder in the Storage navigation tree to display the initiators on your device.
- Step 5** Click the host to which you want to grant or restrict access. The host display appears in the right-hand frame of the interface.
- Step 6** Click the **Targets** tab in the host display.
- Step 7** In the Targets visible to this host table, locate the target that you want the initiator to access, then double-click that row in the table. The IT Properties window opens.
- Step 8** Click the “...” button next to the Port Mask field. The Select Port(s) window opens and displays port numbers for each slot in the chassis. Raised port numbers represent restricted ports. Pressed port numbers represent accessible ports.
- Step 9** Click one or more raised ports to grant the initiator access to the target through those ports.
- Step 10** Click the **OK** button in the Select Port(s) window, then click the **Apply** button in the ITL Properties window and close the window.
- Step 11** Click the **LUN Access** tab.

- Step 12** Expand the gateway icon and the appropriate target icon in the Accessible LUNs field, then click the LUN icon of the LUN that you want the initiator to access.



**Note** If you want to grant port-mask access to a currently inaccessible LUN, use the Available LUNs field.



**Note** The LUN icon appears gray if no SRP host has connected to it.

- Step 13** Click the **Edit ITL Properties** button. The ITL Properties window opens.
- Step 14** Click the “...” button next to the Port Mask field. The Select Port(s) window opens and displays two port numbers for each slot in the chassis. Raised port numbers represent restricted ports. Pressed port numbers represent accessible ports.
- Step 15** Click one or more raised ports to grant the initiator access to the LUN through those ports.
- Step 16** Click the **OK** button in the Select Port(s) window, then click the **Apply** button in the IT Properties window.

## Denying Port Access with Element Manager

To deny an initiator access to a target and LUN through a Fibre Channel gateway port, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Launch Element Manager, and connect to your server switch.
- Step 3** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
- Step 4** Expand the **SRP Hosts** folder in the Storage navigation tree to display the initiators on your device.
- Step 5** Click the host to which you want to grant or restrict access. The host display appears in the right-hand frame of the interface.
- Step 6** Click the **Targets** tab in the host display.
- Step 7** In the Targets visible to this host table, locate the target that you want the initiator to access, then double-click that row in the table. The IT Properties window opens.
- Step 8** Click the button with three dots “...” next to the Port Mask field. The Select Port(s) window opens and displays port numbers for each slot in the chassis. Raised port numbers represent restricted ports. Pressed port numbers represent accessible ports.
- Step 9** Click one or more pressed ports to deny the initiator access to the target through those ports.
- Step 10** Click the **OK** button in the Select Port(s) window, then click the **Apply** button in the ITL Properties window and close the window.
- Step 11** Click the **LUN Access** tab.
- Step 12** Expand the gateway icon and the appropriate target icon in the Accessible LUNs field, then click the LUN icon of the LUN that you want the initiator to access.

**Note**

If you want to grant access to a currently inaccessible LUN, use the Available LUNs field.

**Note**

The LUN icon appears gray if no SRP host has connected to it.

- Step 13** Click the **Edit ITL Properties** button. The ITL Properties window opens.
- Step 14** Click the button with three dots “...” next to the Port Mask field. The Select Port(s) window opens and displays two port numbers for each slot in the chassis. Raised port numbers represent restricted ports. Pressed port numbers represent accessible ports.
- Step 15** Click one or more pressed ports to deny the initiator access to the LUN through those ports.
- Step 16** Click the **OK** button in the Select Port(s) window, then click the **Apply** button in the IT Properties window.

## Granting Port Access with the CLI

To grant an initiator Fibre Channel gateway-port access to a LUN through a target port, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 3** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 4** Enter the configure terminal command to enter Global Configuration mode.

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

- Step 5** Enter the **no fc srp it** command with

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target
- the **gateway-portmask-policy** keyword
- the **restricted** keyword
- the **all** keyword or the ports you want to unmask

to grant the initiator portmask-policy access to the target through the port that you entered.

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

- Step 6** Enter the **no fc srp itl** command with
- the GUID of the host
  - the GUID extension of the host
  - the WWPN of the target
  - the LUN ID of the storage disk
  - the **gateway-portmask-policy** keyword
  - the **restricted** keyword
  - the **all** keyword or the ports you want to unmask

to grant the initiator portmask-policy access to the LUN through the port that you entered.

```
SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

## Denying Port Access with the CLI

To deny an initiator Fibre Channel gateway-port access to a LUN through a target port, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.
- ```
Login: super
Password: xxxxxx
```
- Step 3** Enter the **enable** command to enter Privileged Exec mode.
- ```
SFS-3012R> enable
SFS-3012R#
```
- Step 4** Enter the **configure terminal** command to enter Global Configuration mode.
- ```
SFS-3012R# configure terminal
SFS-3012R(config)#
```
- Step 5** Enter the **fc srp it** command with
- the GUID of the host
 - the GUID extension of the host
 - the WWPN of the target
 - the **gateway-portmask-policy** keyword
 - the **restricted** keyword
 - the **all** keyword or the ports you want to mask

to deny the initiator portmask-policy access to the target via the port that you entered.

```
SFS-3012R(config)# no fc srp it 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab gateway-portmask-policy restricted all
```

- Step 6** Enter the **fc srp itl** command with
- the GUID of the host
 - the GUID extension of the host
 - the WWPN of the target
 - the LUN ID of the storage disk
 - the **gateway-portmask-policy** keyword
 - the **restricted** keyword
 - the **all** keyword or the ports you want to unmask

to deny the initiator portmask-policy access to the LUN via the port that you entered.

```
SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 gateway-portmask-policy restricted all
```

Viewing Port Access Settings

View LUN access settings to verify changes or to troubleshoot connectivity problems. When you view port access settings, you view the ports on your server switch that you have configured to permit the initiator to access the LUN.

Viewing Port Mask Settings with Element Manager

To view portmask access settings, perform the following steps:

-
- Step 1** Launch Element Manager, and connect to your server switch.
- Step 2** From the FibreChannel menu, select SRP. The SRP window opens.
- Step 3** Click the ITL tab. The *GatewayPortMaskPolicy* column lists the ports through which the initiator can access the LUN.
-

Viewing Port Masking Settings with the CLI

To view portmask access settings, perform the following steps:

-
- Step 1** Open a CLI session, and log in.

```
Login: super
Password: xxxxxx
```

Step 2 Enter the **show fc srp itl** command with

- the GUID of the initiator whose port access you want to verify
- the GUID extension of the initiator (always 00:00:00:00:00:00:00:00)
- the WWPN of the target that contains the LUN
- the Fibre Channel LU ID of the LUN

to display the ports that let the initiator access the LUN. The ports that let the initiator connect to the LUN appear in the **non-restricted-ports** field.

```
SFS-3012R# show fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00
```

```
=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
                        description: itl
                        device-category: random
                        lun-policy: non restricted
non-restricted-ports: 2/1-2/2,3/1-3/2,4/1-4/2,5/1-5/2,
                        : 6/1-6/2,7/1-7/2,8/1-8/2,9/1-9/2,
                        : 10/1-10/2,11/1-11/2,12/1-12/2,
                        : 13/1-13/2,14/1-14/2
                        active-ports: 6/1
                        physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
                        dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
                        active-slots: none
```

```
SFS-3012R#
```

Configuring LUN Access on Existing ITLs

When you restrict global LUN access, new ITLs cannot access any storage until you grant them LUN access. When you grant global LUN access, you must restrict LUN access on an individual basis if you do not want your initiator to access all storage.

Granting LUN Access on an ITL with Element Manager

To grant an initiator access to a LUN, perform the following steps:

-
- Step 1** Log in to your host.
 - Step 2** Launch Element Manager, and connect to your server switch.
 - Step 3** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
 - Step 4** Expand the **SRP Hosts** folder in the Storage navigation tree to display the initiators on your device.
 - Step 5** Click the host to which you want to grant or restrict access. The host display appears in the right-hand frame of the interface.
 - Step 6** Click the **LUN Access** tab in the host display.
 - Step 7** Expand all expandable icons in the Available LUNs field and the Accessible LUNs field.
 - Your server switch denies the initiator access to LUNs that appear in the Available LUNs field.
 - Your server switch grants the initiator access to LUNs that appear in the Accessible LUNs field.

In the **Available LUNs** field, you can expand the Inactive ITLs folder to display target icons, then expand target icons to display inactive LUN icons. In the **Accessible LUNs** field, you can expand gateway icons to display target icons, then expand target icons to display active LUN icons and inactive LUN icons.

- Step 8** (Optional) Click a LUN in the Available LUNs field, then click the **Add >** button to grant the initiator access to the LUN.



Note Click a target icon, then the **Add >** button to grant the initiator access to all LUNs in a target. Press-and-hold the **Ctrl** button and click multiple icons, then the **Add >** button to grant the initiator access to the entire selection. Click the **Add All >>** button to grant the initiator access to all available LUNs.

- Step 9** Click the **Apply** button.
 - Step 10** Click the **Refresh** button in the Topspin Storage Manager window.
-

Denying LUN Access on an ITL with Element Manager

To deny an initiator access to a LUN, perform the following steps:

-
- Step 1** Log in to your host.
 - Step 2** Launch Element Manager, and connect to your server switch.
 - Step 3** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.

- Step 4** Expand the **SRP Hosts** folder in the Storage navigation tree to display the initiators on your device.
- Step 5** Click the host to which you want to grant or restrict access. The host display appears in the right-hand frame of the interface.
- Step 6** Click the **LUN Access** tab in the host display.
- Step 7** Expand all expandable icons in the Available LUNs field and the Accessible LUNs field.
- Your server switch denies the initiator access to LUNs that appear in the Available LUNs field.
 - Your server switch grants the initiator access to LUNs that appear in the Accessible LUNs field.
- In the Available LUNs field, you can expand the Inactive ITLs folder to display target icons, and then expand target icons to display inactive LUN icons. In the **Accessible LUNs** field, you can expand gateway icons to display target icons, and then expand target icons to display active LUN icons and inactive LUN icons.
- Step 8** (Optional) Click a LUN in the **Accessible LUNs** field, then click the **Remove >** button to deny the initiator access to the LUN.
-  **Note** Click a target icon, then the **Remove >** button to deny the initiator access to all LUNs in a target. Press-and-hold the **Ctrl** button and click multiple icons, then the **Remove >** button to deny the initiator access to the entire selection. Click the **Remove All >>** button to deny the initiator access to all available LUNs.
- Step 9** Click the **Apply** button.
- Step 10** Click the **Refresh** button in the Topspin Storage Manager window.

Granting LUN Access on an ITL with the CLI

To grant an initiator access to a LUN, perform the following steps:

- Step 1** Log in to your host.
- Step 2** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.
- Login: **super**
Password: **xxxxxx**
- Step 3** Enter the **enable** command to enter Privileged Exec mode.
- ```
SFS-3012R> enable
SFS-3012R#
```
- Step 4** (Optional) Enter the **show fc srp itl** command to display active and inactive ITLs and record
- The GUID of the initiator to which you want to grant or deny access.
  - The WWPN of the target to which you want to grant or deny the initiator access.
  - The fc-lunid of the LUN to which you want to grant or deny the initiator access.
- ```
SFS-3012R# show fc srp itl
```

```

=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
                        description: itl
                        device-category: random
                        lun-policy: restricted
non-restricted-ports: none
active-ports: none
physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
                        active-slots: none

```

Total: 1 itls.

SFS-3012R#

Step 5 Enter the **configure terminal** command to enter Global Configuration mode.

```

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

```

Step 6 (Optional) Enter the **no fc srp itl** command with

- the GUID of the host
- the GUID extension of the host (always **00:00:00:00:00:00:00:00**)
- the WWPN of the target (from <Link>step 4)
- the LUN ID of the storage disk (from <Link>step 4)
- the **lun-policy** keyword
- the **restricted** keyword

to grant the initiator access to the LUN.

```

SFS-3012R(config)# no fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted

```

Denying LUN Access on an ITL with the CLI

To deny an initiator access to a LUN, perform the following steps:

Step 1 Log in to your host.

Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

Step 2 Enter the **enable** command to enter Privileged Exec mode.

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

Step 3 (Optional) Enter the **show fc srp itl** command to display active and inactive ITLs and record

- The GUID of the initiator to which you want to grant or deny access.
- The WWPN of the target to which you want to grant or deny the initiator access.
- The fc-lunid of the LUN to which you want to grant or deny the initiator access.

```
SFS-3012R# show fc srp itl
```

```
=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
                        description: itl
                        device-category: random
                        lun-policy: restricted
                        non-restricted-ports: none
                        active-ports: none
                        physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
                        dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
                        active-slots: none

Total: 1 itls.

SFS-3012R#
```

Step 4 Enter the **configure terminal** command to enter Global Configuration mode.

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

Step 5 (Optional) Enter the **fc srp itl** command with

- the GUID of the host
- the GUID extension of the host (always **00:00:00:00:00:00:00:00**)
- the WWPN of the target Step 4
- the LUN ID of the storage disk (from <Link>step 4)
- the **lun-policy** keyword
- the **restricted** keyword

to deny the initiator access to the LUN.

```
SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 lun-policy restricted
```

Viewing LUN Access Settings

View LUN access settings to verify changes or to troubleshoot connectivity problems. When you view LUN access settings, you view whether or not LUNs let the initiator access them.

Viewing LUN Access with Element Manager

To view LUN access settings, perform the following steps:

-
- Step 1** Launch Element Manager, and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
 - Step 3** Expand the **SRP Hosts** folder in the Storage navigation tree to display the initiators on your device.
 - Step 4** Click the host whose LUN access you want to view. The host display appears in the right-hand frame of the interface.
 - Step 5** Click the **LUN Access** tab, then expand the icons in the Accessible LUNs field. The initiator can access the LUNs in the Accessible LUNs field. The initiator cannot access LUNs in the Available LUNs field.
-

Viewing LUN Access with the CLI

To view LUN access settings, perform the following steps:

-
- Step 1** Open a CLI session, and log in.

```
Login: super
Password: xxxxxx
```

Step 2 Enter the **show fc srp itl** command with

- the GUID of the initiator whose LUN access you want to verify
- the GUID extension of the initiator (always 00:00:00:00:00:00:00)
- the WWPN of the target that contains the LUN
- the Fibre Channel LU ID of the LUN

to display the access between the initiator and the LUN. The access that the initiator has to the LUN appears in the **lun-policy** field.

```
SFS-3012R# show fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00
```

```
=====
                        SRP ITL
=====
                        guid: 00:05:ad:00:00:01:29:c5
                        extension: 00:00:00:00:00:00:00:00
                        target-wwpn: 21:00:00:04:cf:f6:c2:ab
                        fc-lunid: 00:00:00:00:00:00:00:00
                        srp-lunid: 00:00:00:00:00:00:00:00
logical-id (raw 64 bytes): 01:03:00:08:20:00:00:04:cf:f6:c2:ab:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
                        : 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
logical-id (formatted display): 2000000000000000
                        description: itl
                        device-category: random
                        lun-policy: non restricted
non-restricted-ports: 2/1-2/2,3/1-3/2,4/1-4/2,5/1-5/2,
                        : 6/1-6/2,7/1-7/2,8/1-8/2,9/1-9/2,
                        : 10/1-10/2,11/1-11/2,12/1-12/2,
                        : 13/1-13/2,14/1-14/2
                        active-ports: 6/1
                        physical-access: 6/1
                        hi-mark: 16
                        max-retry: 5
                        min-io-timeout: 10
                        dynamic-path-affinity: false
dynamic-gateway-port-loadbalancing: true
dynamic-storage-port-loadbalancing:
dynamic-gateway-port-failover: false
dynamic-storage-port-failover:
                        active-slots: none
```

```
SFS-3012R#
```

Configuring Individual ITL Attributes

Every ITL attribute that you can configure globally (see the [“Configuring Global Attributes”](#) section on [page 3-1](#)), you can also configure individually to customize ITLs after you create them.

Configure the minimum I/O timeout of an ITL to suit the performance of your storage device.

To configure this attribute, perform the following steps:

- Step 1** Launch Element Manager, and connect to your server switch.
- Step 2** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
- Step 3** Expand the **Logical Units** folder and click the LUN that you want to configure.
- Step 4** In the Min IO Timeout field, enter an integer value (seconds) between 1 and 1800, and then click the **Apply** button.

To configure this attribute, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp lu** command with

- the Logical ID of the LUN that you want to configure
- the **min-io-timeout** keyword
- the value that you want to apply

to configure the minimum I/O timeout of the ITL.

[illegible]

Configure dynamic failover to leave one port on a gateway dormant to adopt traffic in the event that the second port on the gateway fails.

To configure this attribute, perform the following steps:

- Step 1** Launch Element Manager, and connect to your server switch.
- Step 2** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
- Step 3** Expand the **Logical Units** folder and click the LUN that you want to configure.
- Step 4** In the Dynamic Pathing field, click the **Gateway Port Failover** radio button, and then click the **Apply** button.

To configure this attribute, perform the following steps:

- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp lu** command with

- the Logical ID of the LU that you want to configure
- the **dynamic-gateway-port-failover** keyword

to enable dynamic port failover and disable path affinity and load balancing.

[illegible]

Configuring ITL Description

Configure an ITL description to assign an easily recognizable identifier to an ITL.

Using Element Manager

To configure this attribute, perform the following steps:

-
- Step 1** Launch Element Manager, and connect to your server switch.
 - Step 2** From the FibreChannel menu, select **Storage Manager...** The Storage Manager window opens.
 - Step 3** Expand the **Logical Units** folder and click the LUN that you want to configure.
 - Step 4** In the Description field, enter a text description, then click the **Apply** button.
-

Using the CLI

To configure this attribute, perform the following steps:

-
- Step 1** Open a CLI session, and log in as a user with Fibre Channel read-write privileges. For more information about privileges, refer to the *Cisco SFS Product Family Command Reference*.

```
Login: super
Password: xxxxxx
```

- Step 2** Enter the **enable** command to enter Privileged Exec mode.

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

- Step 3** Enter the **configure terminal** command to enter Global Configuration mode.

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

- Step 4** Enter the **fc srp itl** command with

- the GUID of the initiator of the ITL that you want to configure
- the GUID extension (always **00:00:00:00:00:00:00:00**)
- the WWPN of the target of the ITL that you want to configure
- the Fibre Channel LU ID (the LUN) of the ITL that you want to configure
- the **description** keyword
- an ASCII description enclosed in quotation marks

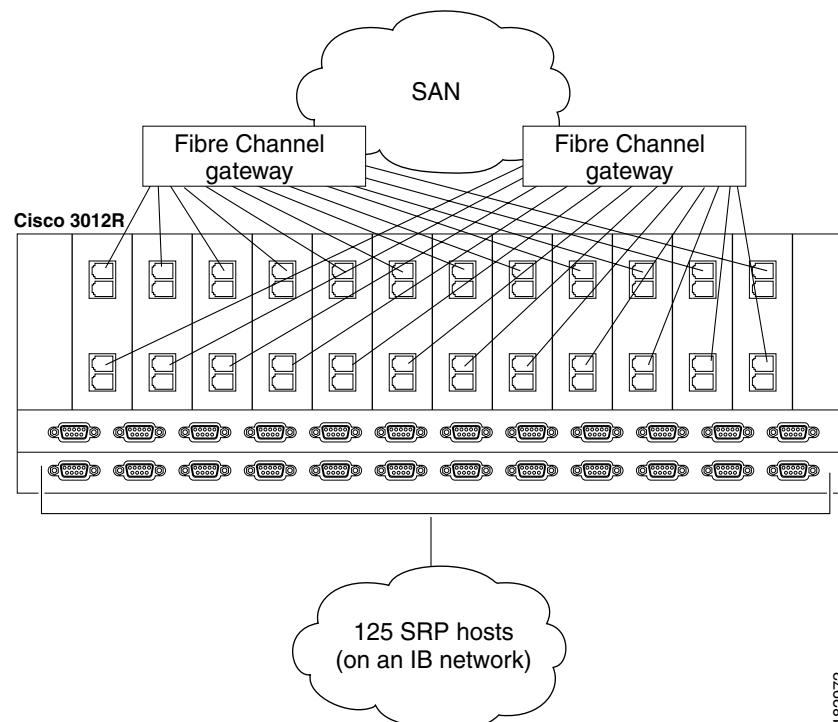
to assign a text identifier to the ITL.

```
SFS-3012R(config)# fc srp itl 00:05:ad:00:00:01:29:c5 00:00:00:00:00:00:00:00
21:00:00:04:cf:f6:c2:ab 00:00:00:00:00:00:00:00 description "my-ITL"
SFS-3012R(config)#
```

Gateway Grouping

Gateway grouping prevents your SRP hosts and Fibre Channel gateways from overloading your Fibre Channel switch with log-ins. Certain Fibre Channel switches may not be able to handle the number of SRP hosts that you want to connect to the SAN.

Figure 5-1 High Node-Count System



In this example, 125 InfiniBand SRP hosts connect through one Cisco SFS 3012R server switch to the Fibre Channel SAN. Without gateway grouping, each SRP host logs into the SAN through *each Fibre Channel gateway port*. In our example, each Fibre Channel edge switch to which the Cisco SFS 3012R server switch connects can receive 1500 *simultaneous* Fibre Channel log-ins. The SAN as a whole can then receive up to 3000 simultaneous log-ins.

To limit the number of possible simultaneous log-ins to a value that your Fibre Channel switch can support, you must initiate gateway grouping. To group gateways, you must manually configure WWPNs on initiators (avoid auto-binding) and only configure WWPNs for the gateways through which you want the initiator to access the SAN. The sections that follow contrast auto-binding from gateway grouping.

WWPN Overload with Auto Binding

When you configure an initiator and run the recommended **auto-bind** keyword, your Fibre Channel gateway dynamically creates WWPNs for all possible physical routes from the SRP host to the storage. As a result, when multiple Fibre Channel gateways connect to a SAN, each SRP host receives WWPNs for the ports on each gateway, regardless of whether or not you plan to grant the SRP host access to all of the gateways.

WWPN Limits with Gateway Grouping

When you manually configure WWPNs (that is, omit the **auto-bind** keyword), you only configure WWPNs on each SRP host for the Fibre Channel gateways that you want to use. As a result, a given SRP host only logs in through the Fibre Channel gateway(s) that you configure it to use, thereby limiting the total number of fabric log-ins.

Manually Configuring with the CLI



Note

You cannot manually assign WWPNs with Element Manager.

To manually configure WWPNs, perform the following steps:

Step 1 Begin to configure ITLs as done in the [“Configuring ITLs” section on page 5-7](#) until you reach the **fc srp initiator** command with the **auto-bind** keyword.

Step 2 Enter the **fc srp initiator** command with

- the GUID of the host
- the GUID extension of the host
- the wwnn keyword
- the WWNN that you want to apply to the SRP host

to assign a WWNN to the SRP host.

```
SFS-3012R(config)# fc srp initiator 00:05:ad:00:00:00:17:17 00:00:00:00:00:00:00 wwnn
20:03:00:05:ad:01:1a:5c
```

Step 3 Enter the **fc srp initiator-wwpn** command with

- the GUID of the SRP host to which you want to assign a WWPN
- the GUID extension of the SRP host
- the slot#/port# of the gateway port to which you want to apply this WWPN
- the WWPN that you want to assign to the port.

to assign WWPNs to virtual ports through Fibre Channel gateway ports.

```
SFS-3012R(config)# fc srp initiator-wwpn 00:05:ad:00:00:00:17:17 00:00:00:00:00:00:00
5/1 20:04:00:05:ad:51:1a:5c
SFS-3012R(config)# fc srp initiator-wwpn 00:05:ad:00:00:00:17:17 00:00:00:00:00:00:00
5/2 20:04:00:05:ad:55:1a:5c
```

Step 4 Continue with ITL configuration as done in the [“Configuring ITLs” section on page 5-7](#).



CHAPTER 6

ITLs and Zoning

The following sections appear in this chapter:

- [Adding Unzoned Initiators \(Fibre Channel Gateway Ports\), page 6-1](#)
- [Configuring RAID Arrays, page 6-2](#)

Introduction

You must add the following to a zone to utilize port name zoning:

- Port names of unzoned initiators (Fibre Channel gateway ports)
- Port names of SRP host initiators (the NL port identifiers that you create when you use the **auto-bind** keyword or the **fc srp initiator-wwpn** command)
- Port names of target devices

Adding Unzoned Initiators (Fibre Channel Gateway Ports)

To identify the WWPN of each Fibre Channel gateway port with the CLI, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Open a CLI session. |
| Step 2 | Enter the show interface fc command with the slot#/port# identifier of the port. |
| Step 3 | Locate the WWPN of the port in the wwpn field of the output. |
-

To identify the WWPN of each Fibre Channel gateway port with Element Manager, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Launch Element Manager. |
| Step 2 | Right-click the port whose WWPN you want to discover, and select Properties . A Fibre Channel Port window opens. |
| Step 3 | Locate the WWPN of the port in the WWPN field. |
-

Adding Initiators

To identify the WWPNs of an initiator with the CLI, perform the following steps:

-
- Step 1** Open a CLI session.
- Step 2** Enter the **show fc srp initiator** command with
- the GUID of the initiator
 - the GUID extension of the initiator
- to display initiator details.
- Step 3** Locate the WWPNs of the initiator in the wwpns section of the output.
-

To identify the WWPNs of an initiator with Element Manager, perform the following steps:

-
- Step 1** Launch Element Manager.
- Step 2** From the FibreChannel menu, select **Storage Manager**.
- Step 3** Expand the **SRP Hosts** folder, and click the host whose ports you want to view.
- Step 4** Click the **General** tab, and locate the WWPNs in the WWPNs table.
-

Verify Zoning

Use the Physical Access column in the targets ports view to see if your zoning worked correctly.

Configuring RAID Arrays

To configure RAID arrays, perform the following steps:

-
- Step 1** Configure the unzoned initiator by configuring an initiator for each port on the gateway. Use the IP address of the chassis.
- Step 2** Configure the individual hosts.
- Step 3** Add the gateway and hosts to storage groups.
-



CHAPTER 7

Configuring PowerPath with a Server Switch

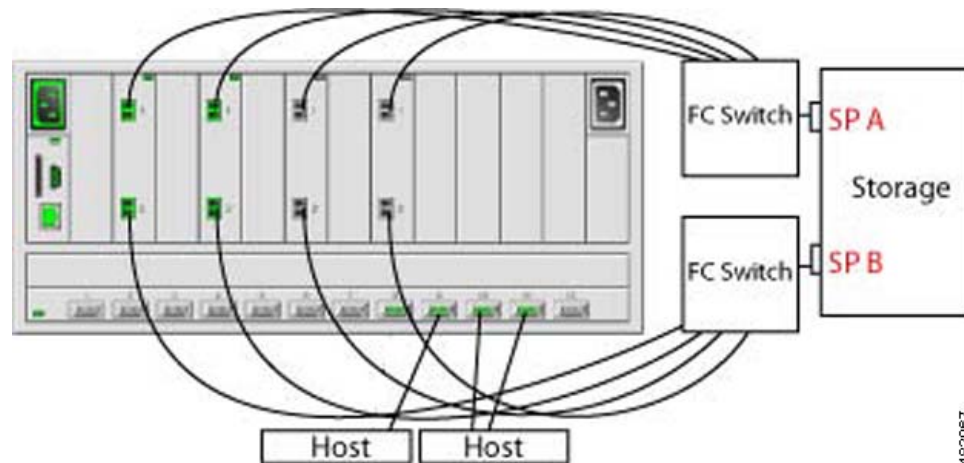
The following sections appear in this chapter:

- [Topology, page 7-1](#)
- [Configuring Fibre Channel Gateway Access to Clariion, page 7-2](#)
- [Configuring SRP Host Access to Clariion, page 7-11](#)

Topology

[Figure 7-1](#) displays the example topology to which the instructions in this chapter refer.

Figure 7-1 Example Topology



Setup

The following status applies to the example setup:

- Two SRP hosts are cabled to the server switch.
- One SRP host has two HCAs, and one port of each HCA connects to the server switch.

- The remaining SRP host has one HCA, and one port on the HCA connects to the server switch.
- All Fibre Channel gateways on the server switch are down.
- Port 1 of each Fibre Channel gateway connects to SP A on the storage system.
- Port 2 of each Fibre Channel gateway connects to SP B on the storage system.
- No SRP hosts have SRP drivers loaded.
- The Cx200 has 33 LUs configured.

The example in this section involved one Cisco SFS 3012R with 4 Fibre Channel gateways. Port 1 of each gateway connects to one Fibre Channel switch, and port 2 on each gateway connects to a second Fibre Channel switch. Each Fibre Channel switch then connects to one port on the EMC Cx200 storage device. The two Fibre Channel switches are not connected in order to maintain two separate fabrics for redundancy and HA.

Introduction

Every single storage port on the Cx200 exports all LUs. Therefore, each gateway sees 66 LUs, not 33. The server switch recognizes that only 33 LUs exist, but the host thinks there are 66. PowerPath sits on top of the SCSI stack and determines that the two appearances actually represent 1 LU with two separate paths to it. If PowerPath detects a path failure, it automatically switches to the other path.

Configuring Fibre Channel Gateway Access to Clariion

To configure grant Fibre Channel gateways access to storage, perform the following steps:

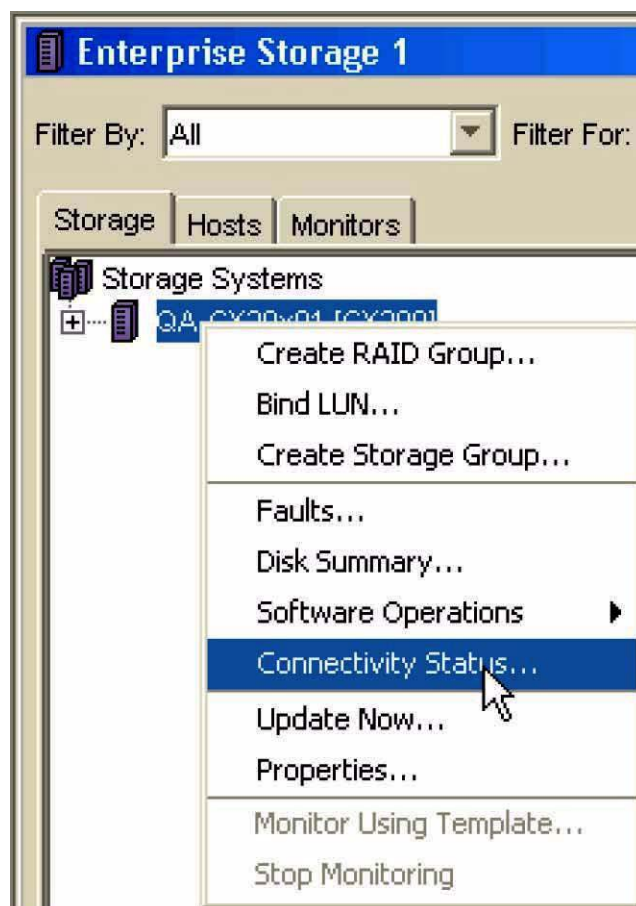
-
- Step 1** Launch your Web browser.
- Step 2** Enter the IP address of your EMC Cx200 in the address bar, and press **Enter** to launch Navisphere.



Note These instructions assume that you have performed all Navisphere prerequisites.

- Step 3** Right-click your storage system, and click **Connectivity Status...** in the right-click menu. The Connectivity Status window opens and displays the initiators that the storage can discover on the Fibre Channel fabrics to which its ports connect. (See [Figure 7-2.](#))

Figure 7-2 Connectivity Status Window Displaying Initiators

**Note**

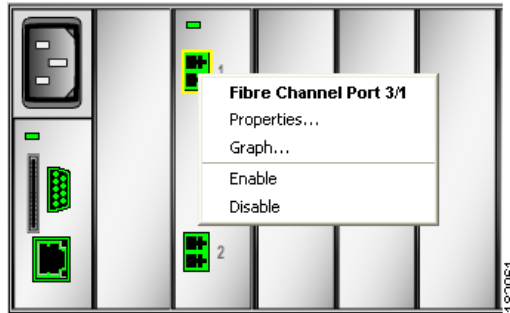
Initiators in the Connectivity Status window do not necessarily have access to the storage device. This window displays only the initiators that the storage discovers on the Fibre Channel fabric to which its storage ports connect. Gateway ports appear consistently connected in this display (if the gateway ports are up). SRP hosts never appear *connected* in the display because they log in to storage as needed but do not remain logged in.

- Step 4** Launch Element Manager, and open the server switch that connects your SRP hosts to your storage.
- Step 5** From the Fibre Channel menu, select **Storage Manager**. The **Storage Manager** window opens.

**Note**

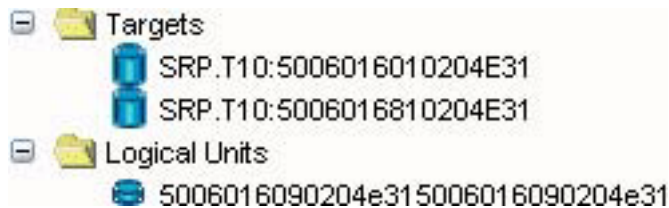
No hosts appear because they have not been configured. No Clariion targets or logical units appear because the gateways are down and the gateway ports have not been configured on the storage.

- Step 6** Check the **Restricted** checkbox in the Gateway Port Access field.
- Step 7** Uncheck the **Restricted** checkbox in the LUN Access field.
- Step 8** Right-click a Fibre Channel gateway card in your initial Element Manager window and select **Properties...** from the right-click menu. A Fibre Channel Card window opens. (See [Figure 7-3](#).)

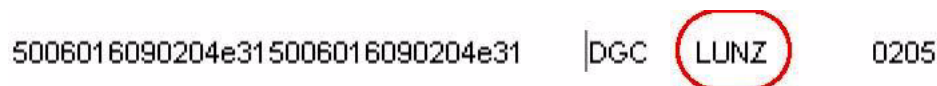
Figure 7-3 Fibre Channel Card Window

Step 9 Click the **up** radio button, then click **Apply** and close the window, and then wait for the gateway to boot.

Step 10 Return to Storage Manager, click the **Reset** button, and expand the **Targets** and **Logical Units** folders. Two targets appear (one for each port on the storage device). One logical unit, “LUN Z,” appears. [Figure 7-4](#) displays LUN Z and both targets.

Figure 7-4 Two Targets and One LUN (LUN Z) in Storage Manager

[Figure 7-5](#) displays LUN Z in the Element Manager SRP display.

Figure 7-5 LUN Z Entry

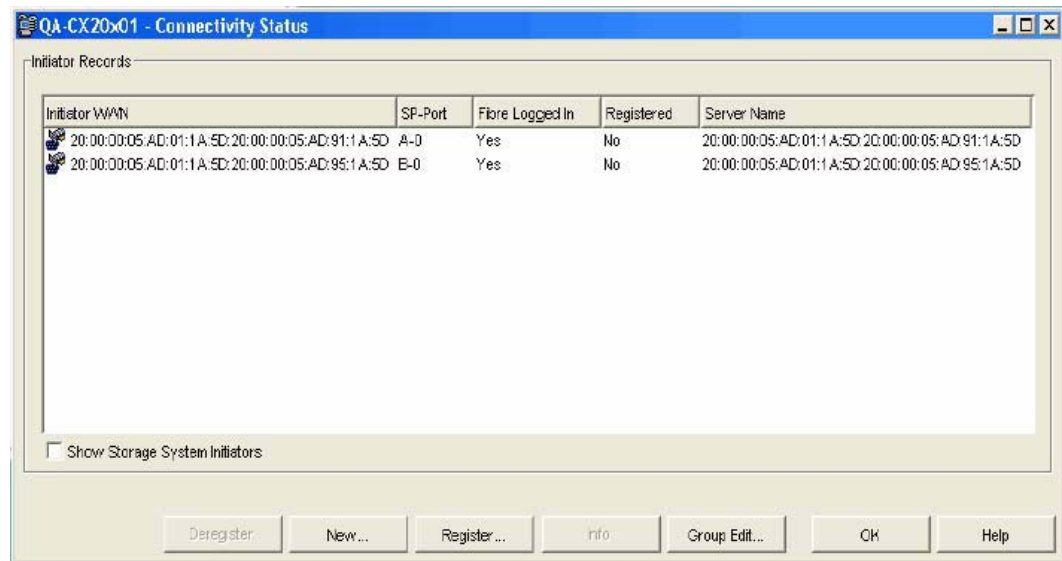
Note Until you add *both* the ports of a gateway and the LUs of the storage to a storage group (below), the gateway sees LUN Z only. The Fibre Channel gateway discovers the two storage ports, but since access to LUs in the storage is restricted by default, only LUN Z appears. LUN Z is not a real LUN and does not run traffic.

Step 11 Return to Navisphere.

Step 12 Right-click your storage device, and click **Connectivity Status...** in the right-click menu. Each port of the gateway that you brought up in <Link>step 9 appears in the Connectivity Status window with a blue icon next to it. In the Server Name column, the world-wide name (WWN) of the port appears. (See [Figure 7-6](#).)



Note The WWN consists of the WWNN of the Fibre Channel gateway port, a colon (:), and the WWP of the Fibre Channel gateway port.

Figure 7-6 Fibre Channel Gateway Ports in Connectivity Status Window

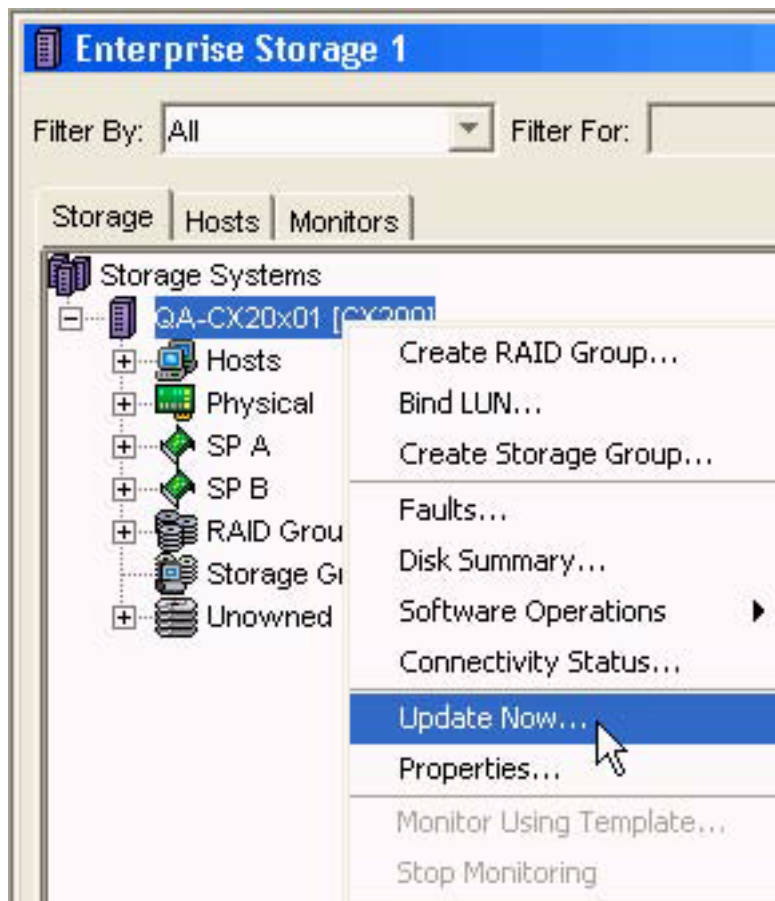
- Step 13** In the Connectivity Status window, click the entry for Port 1 (in our topology, Port 1 always connects to SP port A) of the Fibre Channel gateway, then click the **Register...** button. The Register Initiator Record window opens. (See [Figure 7-7](#).)

Figure 7-7 Register Initiator Record Window

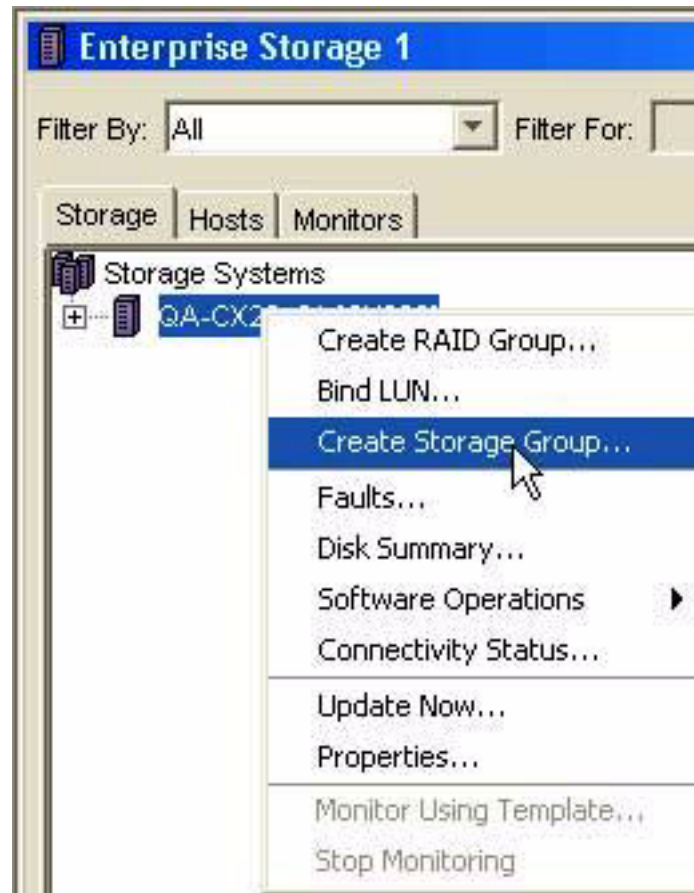
- Step 14** In the Host Name field, assign a host name that identifies the Fibre Channel gateway port by gateway number and port number.

- Step 15** In the IP Address field, enter an IP address. We recommend the IP address of the server switch of the gateway port.
- Step 16** (Optional, Recommended) Select **1** from the Failover Mode pulldown menu.
- Step 17** Click **OK**, and then confirm all dialog boxes until you return to the Connectivity Status window.
- Step 18** Repeat Step 13 through Step 17 through for the second port on the Fibre Channel gateway.
- Step 19** Click **OK** to close the Connectivity Status window.
- Step 20** Right-click the Storage System, and select **Update Now...** from the right-click menu. (See [Figure 7-8](#).)

Figure 7-8 *Update the Storage System*



- Step 21** Right-click your Storage System, and click **Create Storage Group...** in the right-click menu. The Create Storage Group window opens. (See [Figure 7-9](#).)

Figure 7-9 Create Storage Group Window

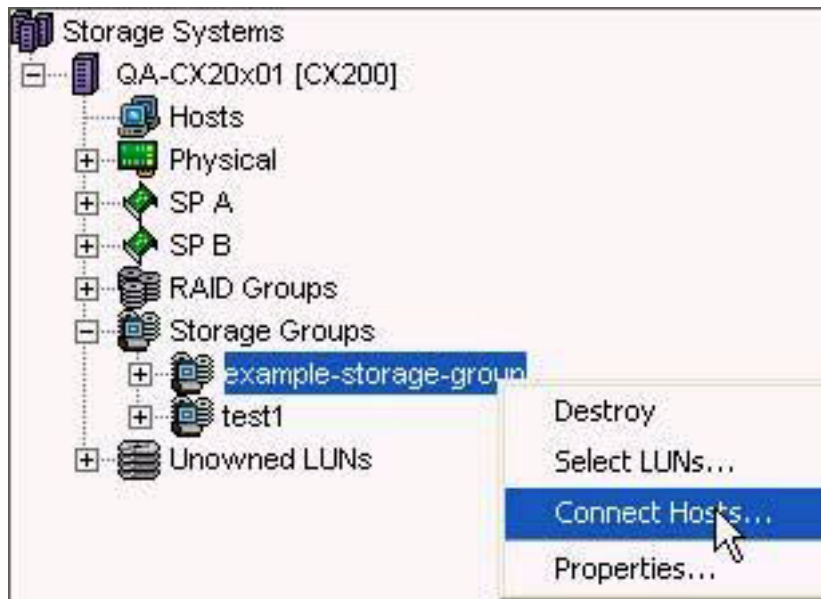
Step 22 In the Storage Group Name field, enter a name for the group, click **OK**, and confirm the dialog boxes, as needed. (See [Figure 7-10](#).)

Figure 7-10 Name the Storage Group

Step 23 Expand your Storage System, and then expand Storage Groups.

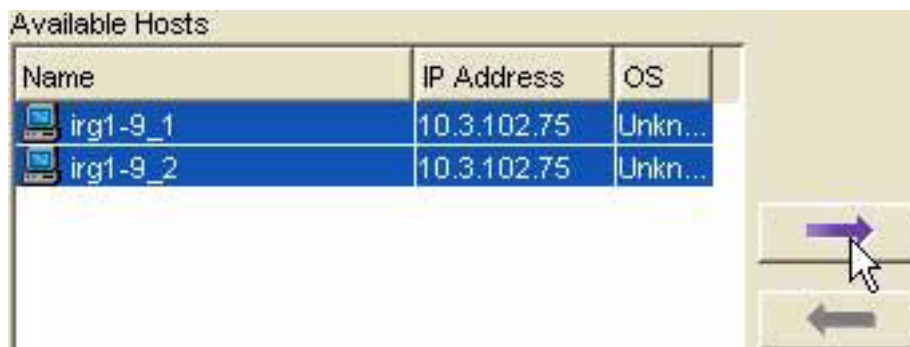
- Step 24** Right-click the storage group that you created, and select **Connect Hosts...** from the right-click menu. (See [Figure 7-11](#).) The Storage Group Properties window opens, and the gateway ports that you configured appear in the Available Hosts field.

Figure 7-11 Storage Group Properties Window

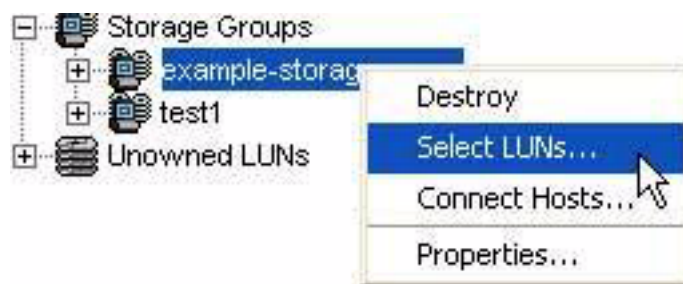


- Step 25** Ctrl-click the two port entries in the Available Hosts field, and then click the right-pointing arrow. (See [Figure 7-12](#).)

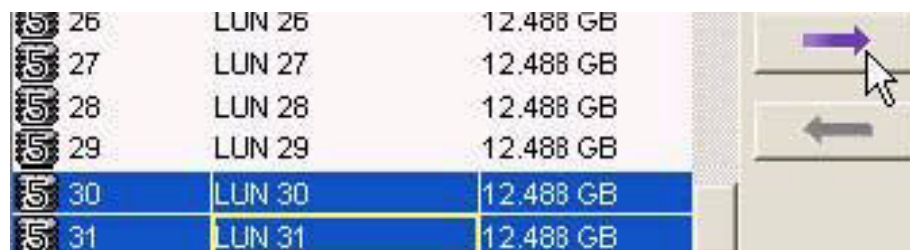
Figure 7-12 Available Hosts



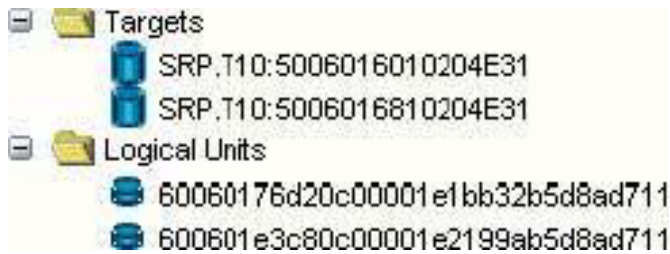
- Step 26** Click **OK**, and then confirm the dialog boxes, as needed.
- Step 27** Right-click the storage group that you created, and select **Select LUNs...** from the right-click menu. (See [Figure 7-13](#).) The Storage Group Properties window opens and the LUs on the Storage System appear in the Available LUNs field.

Figure 7-13 **Select LUNs**

- Step 28** Ctrl-click the LUs that you want to add to the group, and then click the right-pointing arrow. (See [Figure 7-14](#).)

Figure 7-14 **Add LUs to the Group**

- Step 29** Click **OK**, and then confirm the dialog boxes, as needed.
- Step 30** Return to the Element Manager, right-click the Fibre Channel gateway card that you brought up in Step 8, and then select **Properties...** from the right-click menu. A Fibre Channel Card window opens.
- Step 31** Click the **down** radio button, click the **Apply** button, and then close the window.
- Step 32** Return to Storage Manager, and click the Logical Units folder.
- Step 33** Click the **LUNZ** entry in the right-hand Summary panel. The Remove button (on the bottom of the page) becomes active.
- Step 34** Click the **Remove** button to delete LUN Z from the configuration.
- Step 35** Return to Element Manager and right-click the Fibre Channel gateway card that you brought up in Step 8, and then select **Properties...** from the right-click menu. A Fibre Channel Card window opens.
- Step 36** Click the **up** radio button, then click **Apply** and close the window.
- Step 37** Wait for the gateway to come up, then return to Storage Manager and click **Refresh**. The LUs that you added to the Storage Group in Step 28 appear under the Logical Units folder. [Figure 7-15](#) displays the LUs.

Figure 7-15 *New LUs Appear in the Logical Units Folder; LUN Z No Longer Appears*

- Step 38** Repeat Step 8 and Step 9 for all remaining gateways.
- Step 39** Repeat Step 11 through Step 18 through for all remaining gateways.
- Step 40** Return to Navisphere, right-click the storage group, and then select **Connect Hosts...** from the right-click menu.
- Step 41** Ctrl-click all of the hosts in the Host to be Connected field, and then click the left-pointing arrow.
- Step 42** Click **OK**, and then confirm the dialog boxes, as needed.
- Step 43** Right-click the storage group, and then select **Connect Hosts...** from the right-click menu.
- Step 44** Ctrl-click the port entries in the Available Hosts field that you want to connect to the storage, and then click the right-pointing arrow.
- Step 45** Click **OK**, and then confirm the dialog boxes, as needed.
- Step 46** Return to Element Manager, and perform the following steps on each Fibre Channel gateway to bring it down:
- Right-click the Fibre Channel gateway card, and then select **Properties...** from the right-click menu. A Fibre Channel Card window opens.
 - Click the **down** radio button, then click the **Apply** button and close the window.
- Step 47** Return to Storage Manager, and select **SRP...** from the FibreChannel menu. The SRP window opens.
- Step 48** Click the LUs tab.
- Step 49** Click the LUNZ entry, click the **Delete** button to remove the LUNZ entry from the configuration, and then close the SRP window.
- Step 50** Return to the Element Manager, and perform the following steps on each Fibre Channel gateway to bring it up:
- Right-click the Fibre Channel gateway card, and then select **Properties...** from the right-click menu. A Fibre Channel Card window opens.
 - Click the **up** radio button, click the **Apply** button, and then close the window.
- Step 51** Wait for the gateways to boot, return to Storage Manager, click **Refresh**, and then verify that the following are true:
- LUN Z does not appear under the Logical Units folder.
 - The first target is available through Port 1 of all Fibre Channel gateways. (Click the **Targets** folder.)
 - The second target is available through Port 2 of all Fibre Channel gateways.
 - All Logical Units are physically accessible through all Fibre Channel gateway ports. (Click the **Logical Units** folder.)



Note If the LUs are not available through all gateways, perform the following steps to delete and re-create the storage group:

- a. Return to Navisphere.
- b. Right-click the storage group, and then select **Connect Hosts...** from the right-click menu.
- c. Ctrl-click the port entries in the Host to be Connected field, and then click the left-pointing arrow.
- d. Click **OK**, and then confirm the dialog boxes, as needed.
- e. Right-click the storage group and select **Destroy** from the right-click menu.

Step 52 Right-click your Storage System and select **Update Now...** from the right-click menu.

- a. Right-click the Storage System, and select **Create Storage Group...** from the right-click menu. The Create Storage Group window opens.
- b. In the Storage Group Name field, enter a name for the group, click **OK**, and then confirm the dialog boxes, as needed.
- c. Expand your Storage System, and then expand **Storage Groups**.
- d. Right-click the storage group that you created, and select **Connect Hosts...** from the right-click menu. The Storage Group Properties window opens, and the gateway ports that you configured appear in the Available Hosts field.
- e. Ctrl-click the two port entries in the **Available Hosts** field, and then click the right-pointing arrow.
- f. Click **OK**, and then confirm the dialog boxes, as needed.
- g. Right-click the storage group that you created, and select **Select LUNs...** from the right-click menu. The Storage Group Properties window opens, and the LUs on the Storage System appear in the Available LUNs field.
- h. Ctrl-click the LUNs that you want to add to the group, and then click the right-pointing arrow.
- i. Click **OK**, and then confirm the dialog boxes, as needed.
- j. Reboot all Fibre Channel gateways.
- k. Return to the Storage Manager, and refresh the view. If the display still appears improperly, reboot the Clariion.

Configuring SRP Host Access to Clariion

To configure SRP host access to the Storage System, perform the following steps:

- Step 1** Telnet to your SRP host, and log in.
- Step 2** Enter the **lsmod** command to confirm that no drivers have been loaded.
- Step 3** Load IB drivers, as appropriate, to your platform.
- Step 4** Launch Element Manager, and open the server switch that connects your SRP hosts to your storage.
- Step 5** Verify that the InfiniBand ports that connect to the SRP hosts are active. [Figure 7-16](#) displays an active IB port.

Figure 7-16 Active IB Port

- Step 6** From the Fibre Channel menu, select **Storage Manager**. The Storage Manager window opens.
- Step 7** Click the **SRP Hosts** folder, and then click the **Define New** button (at the bottom of the display). The Define New SRP Host window opens.



Note If your host includes multiple HCAs, you must configure each individual HCA as an initiator. When you configure one HCA in a host, any other HCAs in the host are not automatically configured.

- Step 8** Select your SRP host from the Host GUID pulldown menu.
- Step 9** (Optional, Recommended) Enter a description in the Description field.
- Step 10** Click the **Next >** button, and then click the **Finish** button.

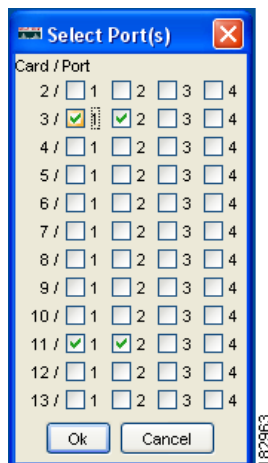


Note If your host includes two HCAs, repeat Step 7 through Step 10 for the second HCA.

- Step 11** Click the new host under the SRP Hosts folder, and then click the **Targets** tab.
- Step 12** Double-click the WWPN, in the Targets visible to this host field, of the target that connects to Port 1 of the Fibre Channel gateways in the server switch. The IT Properties window opens.
- Step 13** Click the “...” button in the Port Mask field. The Select Ports window opens.
- Step 14** Click port **1** for each gateway to which the target connects, and then click the **OK** button. (See [Figure 7-17](#).)



Note Remember, each target connects to *one* Fibre Channel gateway port on each gateway.

Figure 7-17 Select Ports

- Step 15** Click the **Apply** button, and then close the IT Properties window.

- Step 16** Double-click the WWPN, in the Targets visible to this host field, of the target that connects to Port 2 of the Fibre Channel gateways in the server switch. The IT Properties window opens.
- Step 17** Click the “...” button in the Port Mask field. The Select Ports window opens.
- Step 18** Click port **2** for each gateway to which the target connects, and then click the **OK** button.
- Step 19** Return to Navisphere, right-click the Storage System, and select **Connectivity Status...** from the right-click menu.



Note The SRP host that you configured will not appear.

- Step 20** Click the **New...** button. The Create Initiator Record window opens.
- Step 21** In the HBA WWN field, enter the WWNN of the SRP host, then enter a colon (:), and then enter the WWPN of virtual port 1 of a Fibre Channel gateway through which you want to connect the host to the storage. (See [Figure 7-18](#).)

Figure 7-18 Identify WWNN and WWPN

20:01:00:05:AD:01:1A:5D;20:01:00:05:AD:91:1A:5D

SRP Host WWNN ↑ WWPN of SRP Host virtual port
colon



Note To find the WWNN of the SRP host, click the **SRP Hosts** folder in Storage Manager and view the WWNN column in the Summary display. To find the virtual port WWPN, click the **SRP host** under the SRP Hosts folder, then click the **General** tab and view the WWPNs display.

- Step 22** Select **A** from the SP pulldown menu.
- Step 23** Select **1** from the Failover Mode pulldown menu.
- Step 24** Enter a host name in the Host Name field.
- Step 25** Enter the IP address of the SRP host in the IP Address field.
- Step 26** Click **OK**, and then confirm dialog boxes, as needed.
- Step 27** Click the **New...** button. The Create Initiator Record window opens.
- Step 28** In the HBA WWN field, enter the WWNN of the SRP host, then enter a colon (:), and then enter the WWPN of virtual port 2 of the same Fibre Channel gateway as <Link>step 21.
- Step 29** Select **B** from the SP pulldown menu.
- Step 30** Select **1** from the Failover Mode pulldown menu.
- Step 31** Click the **Existing Host** radio button.
- Step 32** Select the host name from Step 24 from the Host pulldown menu.
- Step 33** Click **OK**, and then confirm dialog boxes, as needed.
- Step 34** Repeat Step 20 through Step 33 for all *gateways* through which you want to connect the host.
- Step 35** Close the Connectivity Status window.
- Step 36** Right-click your Storage System, and select **Update Now...** from the right-click menu.

- Step 37** Right-click your storage group, and select **Connect Hosts...** from the right-click menu.
- Step 38** Ctrl-click all hosts in the Host to be Connected field, and click the left-pointing arrow.
- Step 39** Click **OK**, and then confirm dialog boxes as needed.
- Step 40** Right-click the storage group, and select **Connect Hosts...** from the right-click menu.
- Step 41** Ctrl-click the port entries in the Available Hosts field, and then click the right-pointing arrow.
- Step 42** Click **OK**, and then confirm dialog boxes, as needed.
- Step 43** Return to Storage Manager.
- Step 44** Click your host under the SRP Hosts folder, and then click the **Discover LUNs** button under the LUN Access tab. (The Discover LUNs button appears at the bottom of the display.)



Note Your host should discover *twice the number of LUNs that you added to the storage group* in Step 28 of the [“Configuring Fibre Channel Gateway Access to Clariion”](#) section on page 7-2 because the host sees each LUN through each storage port.

- Step 45** Telnet to the host, and load SRP host drivers in the method appropriate for your platform.

```
[root@qa6650-2 root]# modprobe ts_srp_host
```

- Step 46** Wait until the CLI prompt reappears, and then enter the `cat /proc/scsi/scsi` command.

```
[root@qa6650-2 root]# cat /proc/scsi/scsi
Attached devices:
Host: scsi1 Channel: 00 Id: 06 Lun: 00
  Vendor: PE/PV      Model: 1x5 SCSI BP      Rev: 1.1
  Type:   Processor  ANSI SCSI revision: 02
Host: scsi1 Channel: 02 Id: 00 Lun: 00
  Vendor: MegaRAID   Model: LD 0 RAID0   69G Rev: 1.80
  Type:   Direct-Access ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: DGC        Model: RAID 5          Rev: 0205
  Type:   Direct-Access ANSI SCSI revision: 04
Host: scsi2 Channel: 00 Id: 00 Lun: 01
  Vendor: DGC        Model: RAID 5          Rev: 0205
  Type:   Direct-Access ANSI SCSI revision: 04
Host: scsi2 Channel: 00 Id: 01 Lun: 00
  Vendor: DGC        Model: RAID 5          Rev: 0205
  Type:   Direct-Access ANSI SCSI revision: 04
Host: scsi2 Channel: 00 Id: 01 Lun: 01
  Vendor: DGC        Model: RAID 5          Rev: 0205
  Type:   Direct-Access ANSI SCSI revision: 04
```



Note Each appearance of ANSI SCSI revision: 04 represents a LU that the host sees. In the example, four instances appear, which represent the two LUs in the storage group.

- Step 47** Enter the `cd /etc/init.d` command.
- Step 48** Enter the `./PowerPath start` command.
- Step 49** Enter the `powermt display dev=all` command to display paths to the storage LUs and status. Active paths appear as **alive**.

```
[root@qa6650-1 init.d]# powermt display dev=all
Pseudo name=emcpowerac
CLARiion ID=APM00031401737
Logical device ID=60060176D20C00001D1BB32B5D8AD711
```

```

state=alive; policy=CLAROpt; priority=0; queued-IOS=0
=====
----- Host ----- - Stor - -- I/O Path - -- Stats ---
### HW Path          I/O Paths  Interf.  Mode   State  Q-IOS  Errors
=====
    2 srp              sdc       SP A0    active  alive    0      0
    2 srp              sde       SP B0    active  alive    0      0

Pseudo name=emcpowerad
CLARiion ID=APM00031401737
Logical device ID=600601E3C80C00001E2199AB5D8AD711
state=alive; policy=CLAROpt; priority=0; queued-IOS=0
=====
----- Host ----- - Stor - -- I/O Path - -- Stats ---
### HW Path          I/O Paths  Interf.  Mode   State  Q-IOS  Errors
=====
    2 srp              sdb       SP A0    active  alive    0      0
    2 srp              sdd       SP B0    active  alive    0      0

```

- Step 50** Return to Navisphere, right click the Storage System, and select **Connectivity Status...** from the right-click menu.
- Step 51** Repeat Step 19 through Step 34 for all hosts.
- Step 52** Repeat Step 35 through Step 42.
- Step 53** Perform the following steps for each host that you added in Step 51.
- Return to Storage Manager.
 - Click the host under SRP Hosts folder.
 - Click the **Discover LUNs** button.
- Step 54** Repeat Step 43 through Step 48 for all hosts.



CHAPTER 8

Configuring Hitachi Storage

The following sections appear in this chapter:

- [Sample Topology, page 8-1](#)
- [Installing and Configuring the Storage Application \(DAMP 3\), page 8-2](#)
- [Connecting the Array to the Fibre Channel Gateway, page 8-4](#)
- [Using Host Group Security, page 8-6](#)
- [Managing Host Groups, page 8-6](#)
- [Configuring a RAID Group, page 8-10](#)
- [Adding LUs to a RAID Group, page 8-14](#)
- [Making LUs Visible to Hosts, page 8-15](#)

Sample Topology

The following example describes configuring the following:

- One Cisco SFS 3012R with Fibre Channel gateway or one Cisco SFS 3001 server switch with Fibre Channel gateway.
- Hitachi DF600 with two RAID controllers.

The sample IP addresses for the two controllers on the storage array are as follows:

- 10.2.1.141 for Controller 0
- 10.2.1.142 for Controller 1

Installing and Configuring the Storage Application (DAMP 3)

The Hitachi storage array requires that a specific Java application be installed on your computer before the storage can be configured.

The application is called Disk Array Management Program 3 (DAMP 3). The CD should have come with the storage hardware.

To use the storage application, perform the following steps:

-
- Step 1** Install and launch the DAMP 3 application.
 - Step 2** Configure a password for the Management Mode.
 - a. Click **Settings > Password** on the menu bar.
 - b. Enter the new password twice, as prompted.
 - c. Click **OK** to set the password for Management Mode.
 - Step 3** Enter Management Mode.
 - a. Click **File > Change Mode** on the menu bar.
 - b. You are asked to enter the password for Management Mode. Enter the password that you just configured. The current mode is visible in a window labeled “Active Mode” on the upper side of the main application window.
 - Step 4** Register the Hitachi storage array.
 - a. Click on the menu bar on **Add > Register Array Unit**. A new window will open into which you can enter information.
 - b. Enter a name for the storage group. The name cannot have spaces.
 - c. Enter a name for the array that you are adding. The name cannot have spaces.
 - d. Select the **Array Unit Type**, which is *DF600 Dual*, in this example.
 - e. Click the **Connection Type**, which is TCP/IP(LAN).
 - f. Specify the IP addresses for the two RAID controllers. (See [Figure 8-1.](#)) In this example, the IP address would be the addresses mentioned in the “[Sample Topology](#)” section on page 8-1.

Figure 8-1 IP Addresses for RAID Controllers

Property

Array Unit

Group Name: group1

Array Unit Name: array1

Array Unit Type: DF600 Dual

Connection Type: ☒ TCP/IP(LAN) ☐ RS232C

IP Address or Host Name

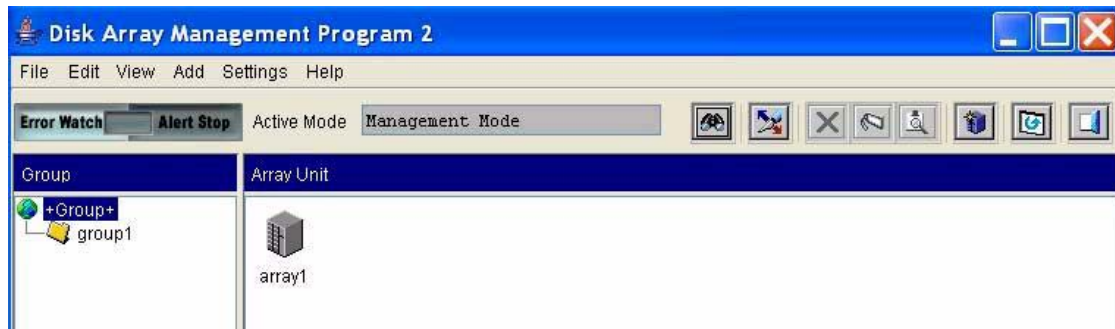
Controller 0: 10.2.1.141

Controller 1: 10.2.1.142

Error Monitoring: ☒ Monitoring Target

- g. Click on **OK**, and wait until the application connects to the storage array. Establishing the connection can take a few minutes.

Step 5 Verify that the application registered with the storage array correctly. The main window right frame will contain a new icon, labeled with the name that you entered for the storage array. (See [Figure 8-2.](#))

Figure 8-2 **New Storage Array**

Connecting the Array to the Fibre Channel Gateway

The storage array may be connected directly to the Fibre Channel gateway, or it may be connected through a Fibre Channel switch.

To connect the array to the Fibre Channel gateway, perform the following steps:

- Step 1** Configure the array port.
- In the Array System Viewer window, select from the menu bar: **Settings > Configuration Settings**.
 - Click the **Fibre Channel** tab.
 - Click the **Port #** in the Controller section.



Note The WWPN for this target is in the Port Name field. You might need to use this information to configure zoning.

- From the drop-down menu in the Topology Information section, choose **Loop** to directly connect to a 2-port gateway, or choose **Point to Point** to connect to a switch.
- Click **Apply**.
- Repeat Step 1 for each Controller and port to which you are connected. (See [Figure 8-3](#).)

Figure 8-3 Configure Array Port as a Loop

Parameter

Array Unit:

Micro Update | Logical Unit Cache | Command Device | RTC | System Parameter | Performance Statistics

Port Option | Unit Identifier | LAN | Restore Options | Online Verify | Constitute | Fibre Channel | Spare Drive | Options

Controller 0: Port 0A | Port 0B | Port 0C | Port 0D

Controller 1: Port 1A | Port 1B | Port 1C | Port 1D

Node Name:

Port Name:

Port Address: Current Value: New Value:

Topology Information: Current Value: New Value:

Transfer Rate: Current Value: New Value:

Security Information: ☐ Security Information Enable

No.	Node Name	Port Name

- Step 2** Verify that the gateway port comes up correctly on the chassis and that the Hitachi target is discovered. LU discovery is not relevant at this point.
- Step 3** You must reset the Fibre Channel gateway port by bringing it down and up if you make any changes to the array Fibre Channel port. For example, if a directly-connected array port is initially configured for Point-to-Point, after you change the setting to Loop, you must disable and then enable the gateway port to see the target.
- Step 4** Click **Apply**, and click **Close**.

After following these steps, the Fibre Channel gateway discovers the array target port to which it is connected (either directly or through any Fibre Channel fabric).



Note If the Fibre Channel gateway does not discover the port to which it is connected, verify that the settings and zone configuration are correct.

Using Host Group Security

Host group security can be enabled on a controller-port basis. When enabled, each initiator's WWNs must be added to a host group to be able to access LUs in that group. The SFS is capable of providing fine-grained access control, so we recommend that you do not use this feature on the array. Disabling host group security will reduce the overall amount of configuration required. However, if your policies require this redundant level of security, you can enable it.

For each port, right-click on the port, and select **Host Group Security > Enable** or select **Host Group Security > Disable**.

Managing Host Groups

If you are using Host Group Security, you must create a host group for each set of hosts for which you want to provide access to the same set of LUs. For example, if you have a set of hosts accessing shared storage, all of these hosts should be in the same host group so that they can access the shared storage. A host group is created on a controller-port basis, so if you want the hosts to access LUs on multiple targets, you also need to create a host group on each controller-port to be used.

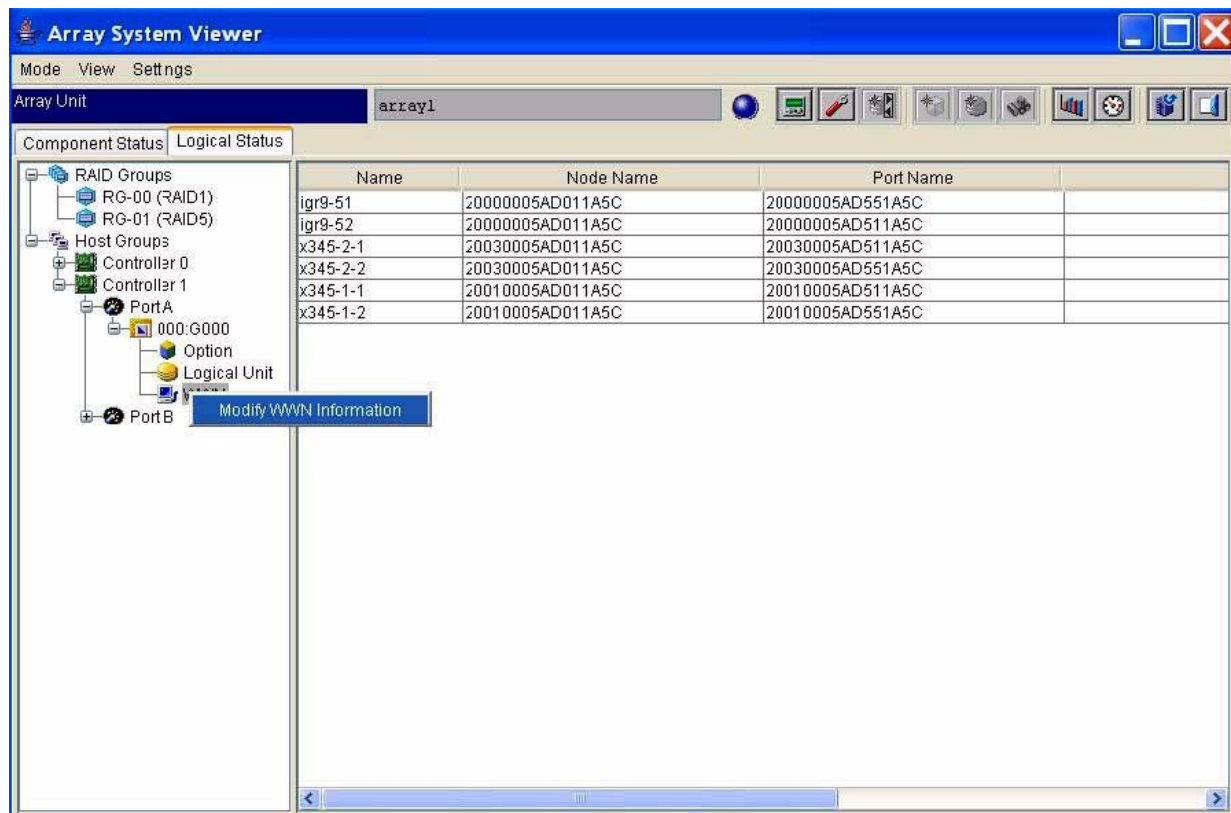
To create a host group and add hosts to the group, follow these steps:

-
- Step 1** From the Logical Status tab in the Array System Viewer, right click on the port to which you want to add a host group, and select **Add a New Host Group**. You can supply your own name or use the default name.

After your host groups are created, you need to add the hosts to the group.

First create the hosts on the SFS switch, and then use the following steps to add the hosts to host groups:

-
- Step 1** In the left side frame of the Array System Viewer window, click open the **Host Groups “+”** folder.
- Step 2** Click open the **Controller “+”** to which you want to connect.
- Step 3** Click open the **Port “+”** to which you want to connect.
- Step 4** Click on the **Group “+”** to which you want to add your host. It will expand into 3 items: Option, Logical Unit, and WWN.
- Step 5** Right-click on **WWN** to add the host WWNs.
- Step 6** Click on **Modify WWN Information**. (See [Figure 8-4](#).)

Figure 8-4 *Modify WWN Information*

Step 7 A new window appears into which you can add the hosts to the list of Assigned WWNs. (See [Figure 8-5](#).)

Figure 8-5 Add Hosts to List

Property

WWN Information

Port: 1A

Host Group: 000:G000

WWN Information

Assigned WWN

Name	Node Name	Port Name
------	-----------	-----------

Add Change Delete

Add

Assignable WWN

Name	Node Name	Port Name
igr9-51	20000005AD011A5C	20000005AD551A5C
igr9-52	20000005AD011A5C	20000005AD511A5C
x345-2-1	20030005AD011A5C	20030005AD511A5C
x345-2-2	20030005AD011A5C	20030005AD551A5C
x345-1-1	20010005AD011A5C	20010005AD511A5C
x345-1-2	20010005AD011A5C	20010005AD551A5C

OK Cancel

Adding WWN

The WWN must be added manually because there is no persistent login to the target for the initiator (unless you enter test mode, as described in the [“Configuring IT Pair Mode for Persistent Binding”](#) section on page 5-6.)

To add the WWN manually, follow these steps:

- Step 1** Obtain the WWN from the Element Manager or the CLI. The WWN is the pair WWNN and WWPNN.
- Step 2** In Element Manager, obtain the WWN by navigating to **Fibre Channel > SRP**.
- Step 3** Click on the **Initiator** tab for the WWN.
- Step 4** Click on the **Initiator WWPNN** tab for the WWPNNs.
- Step 5** Click into the **WWPNN** field to make it selectable. In most cases, you can use this to paste into the DAMP.
- Step 6** Click the **Add** button directly in the Assigned WWN frame. The WWN window appears. (See [Figure 8-6](#).)

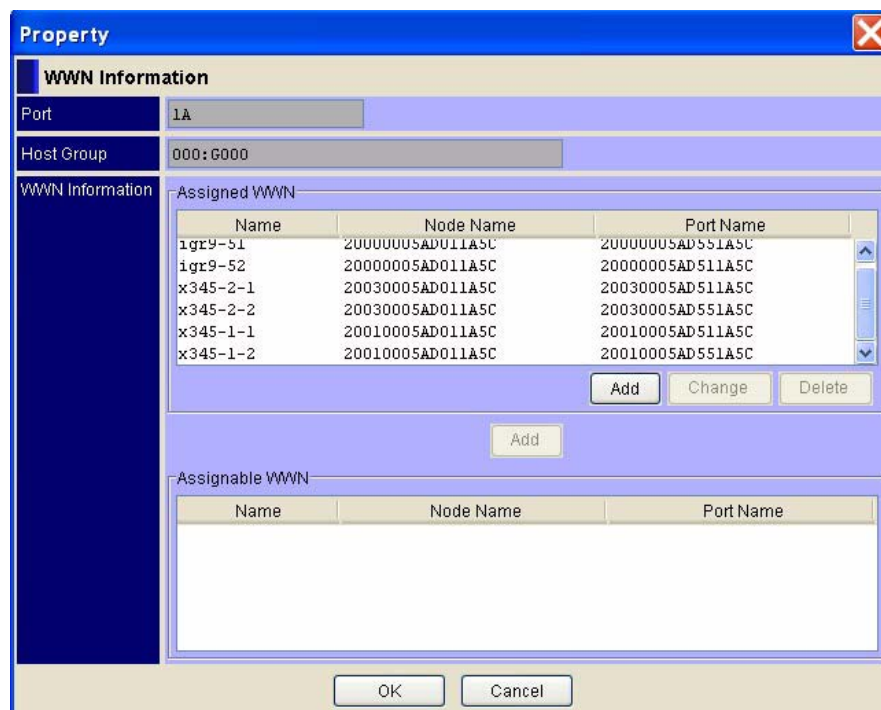
Figure 8-6 *WWN Window*


The WWN Window is a dialog box with a blue title bar and a close button. It contains five input fields and two buttons at the bottom.

Port	1A
Host Group	000:G000
Name	x345-1-1
Node Name	20010005AD011A5C
Port Name	20010005AD511A5C

Buttons: OK, Cancel

- Step 7** Add the name of the host, the WWNN, and the WWPN of the port.
- Step 8** Click **OK**.
- Step 9** Repeat for each WWPN for each host that you want to add to the host group.
- Step 10** Verify that all WWNs of the hosts to be added to this host group are added to the list of Assigned WWNs at the top of the window. (See [Figure 8-7](#).)

Figure 8-7 *Verify that all WWNs Were Added*


The Property window shows the WWN Information tab. It contains a table of Assigned WWNs and a section for Assignable WWNs.

Name	Node Name	Port Name
igr9-51	20000005AD011A5C	20000005AD551A5C
igr9-52	20000005AD011A5C	20000005AD511A5C
x345-2-1	20030005AD011A5C	20030005AD511A5C
x345-2-2	20030005AD011A5C	20030005AD551A5C
x345-1-1	20010005AD011A5C	20010005AD511A5C
x345-1-2	20010005AD011A5C	20010005AD551A5C

Buttons: Add, Change, Delete

Assignable WWN section:

Name	Node Name	Port Name

Buttons: OK, Cancel

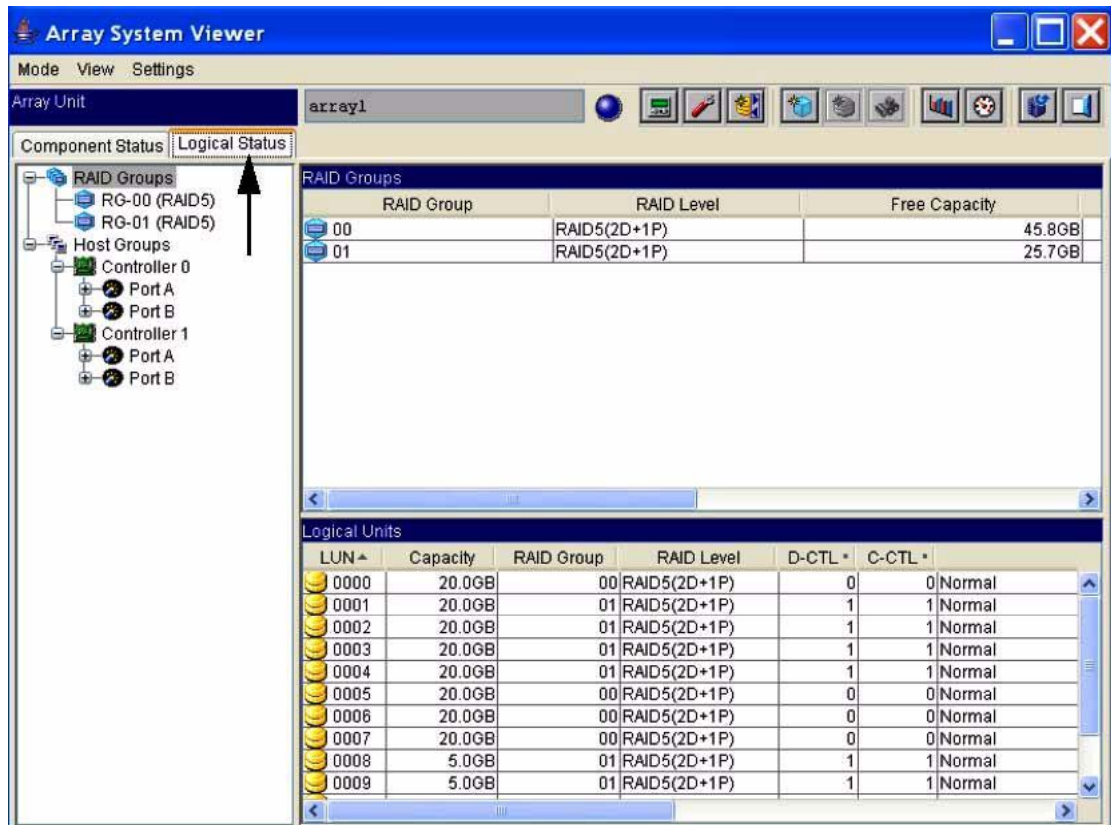
Step 11 After you verify that all assigned WWNs appear, click **OK**.

Configuring a RAID Group

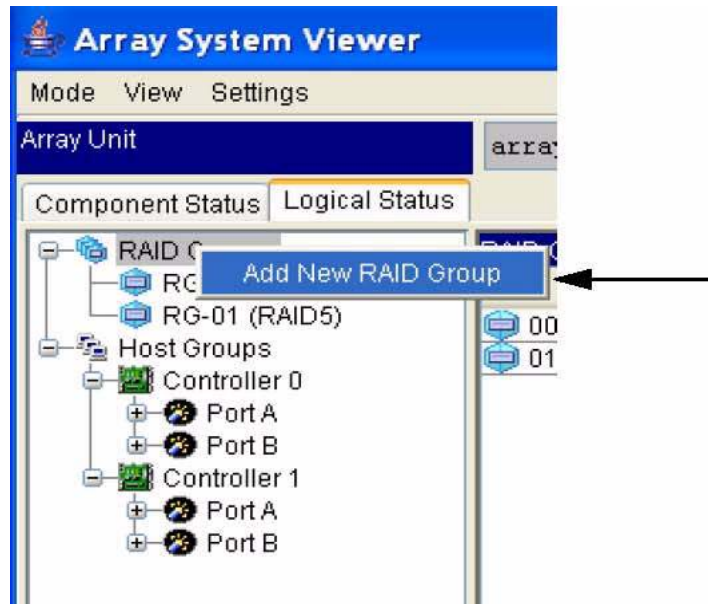
Step 1 Double-click on the new storage icon to open the Array System Viewer window.

Step 2 Click the **Logical Status** tab. (See [Figure 8-8](#).)

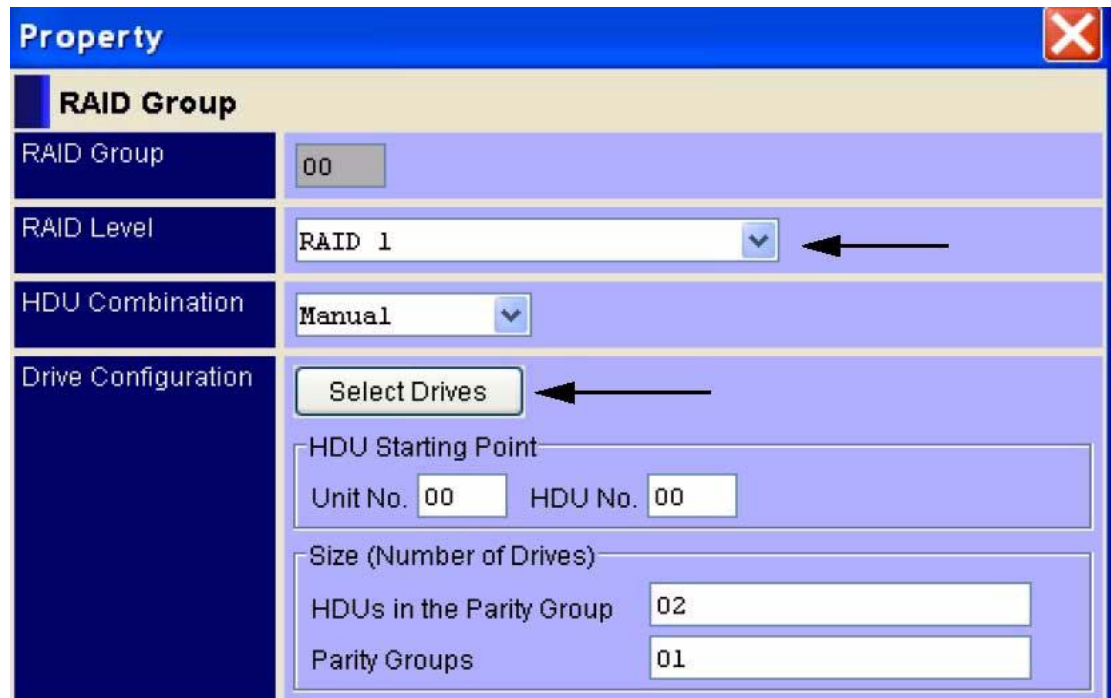
Figure 8-8 Click Logical Statistics Tab



Step 3 In the left side frame of the Array System Viewer window, right click on the **RAID Groups** item, and then select **Add new RAID group**. (See [Figure 8-9](#).)

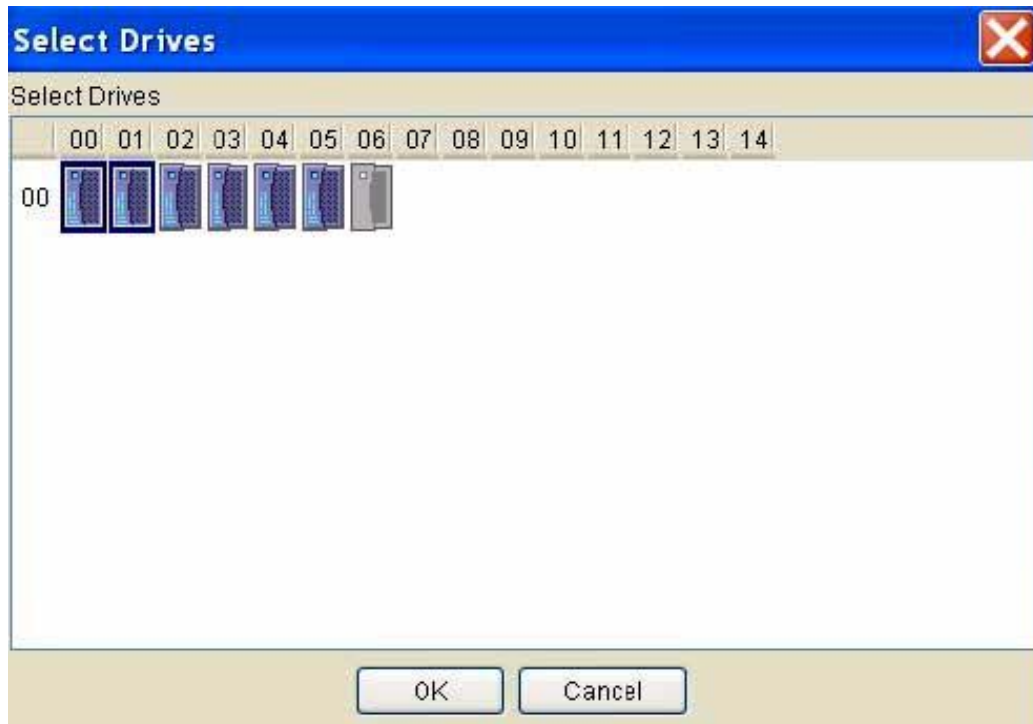
Figure 8-9 Add a New RAID Group

Step 4 A new window opens. Select the RAID Level (usually RAID 5). (See [Figure 8-10](#).)

Figure 8-10 Select RAID Level

Step 5 Locate the Drive Configuration section, and click the **Select Drives** button. The **Select Drives** window appears.

Step 6 Select the physical drives that you want to use in your new RAID group. Hold down the Ctrl key to select multiple drives. (See [Figure 8-11](#).)

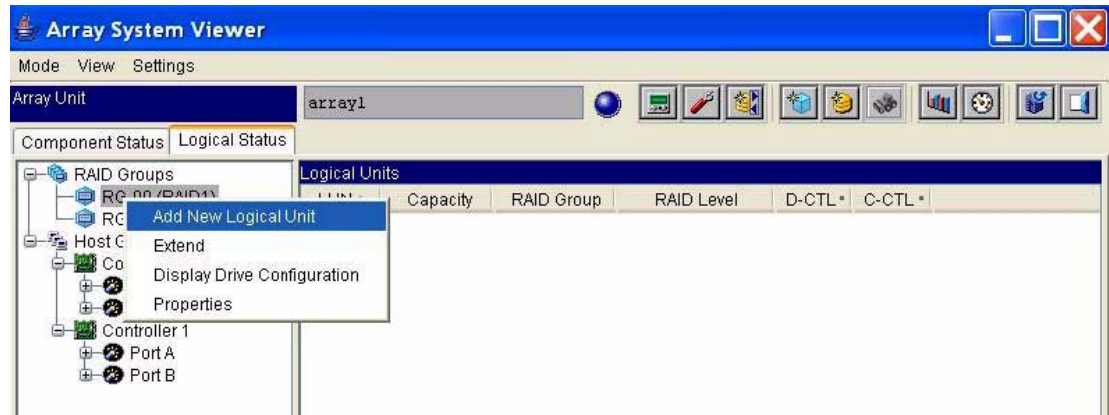
Figure 8-11 **Select Drives**

- Step 7** Click **OK**. The Raid Property window returns, and the rest of the fields in the RAID Group window are automatically filled in for you.
- Step 8** Click **OK** to add the new RAID group.
- Step 9** A message appears stating that the “Setting Ended Normally.” Click **OK**.
-

Adding LUs to a RAID Group

- Step 1** In the left side frame of the Array System Viewer window, right click on the RAID Group to which you want to add an LU, and then select **Add New Logical Unit**. (See [Figure 8-12](#).)

Figure 8-12 Add New Logical Unit



A new window opens.

- Step 2** Select which controller should be the default for this LU.
- Step 3** In the Size section, slide the bar across to select the LU size.
- Step 4** Leave the other parameters as they are unless you have specific reasons not to do so.
- Step 5** Click **OK** to start creating the new LUN.
- Step 6** A message appears stating that the "Setting Ended Normally." Click **OK** to close the LU Property window.
- Step 7** In the left side frame of the Array System Viewer window, right-click on the RAID Group into which you added the new LU. Look in the right side frame for the new LU to appear. The color is grey because the LU is not formatted yet.
- Step 8** In the right frame, right-click on the line containing the new LU, and then select **Format > Online**.



Note You can use Quick format, but the online format is recommended.

- Step 9** Wait until the LU is formatted, which can take a few minutes, depending on the size of your LU. After the formatting process completes and the main window refreshes, the color of your new LU changes from grey to orange to show that the LU is formatted.

Making LUs Visible to Hosts

To make LUs visible to hosts, follow these steps:

- Step 1** In the left side frame of the **Array System Viewer** window, click open the **Host Groups “+”** folder.
- Step 2** Click open the **Controller “+”** to which you want to connect.
- Step 3** Click open the **Port “+”** through which the LUs are exported.
- Step 4** Click on the **Group “+”** to which you want to add LUs. It expands into two or three items: Option, Logical Unit, and WWN. The WWN option will be present only if you are using Host Group Security.
- Step 5** Right-click the **Logical Unit** for this host group.
- Step 6** Click **Modify Mapping**. (See [Figure 8-13](#).)

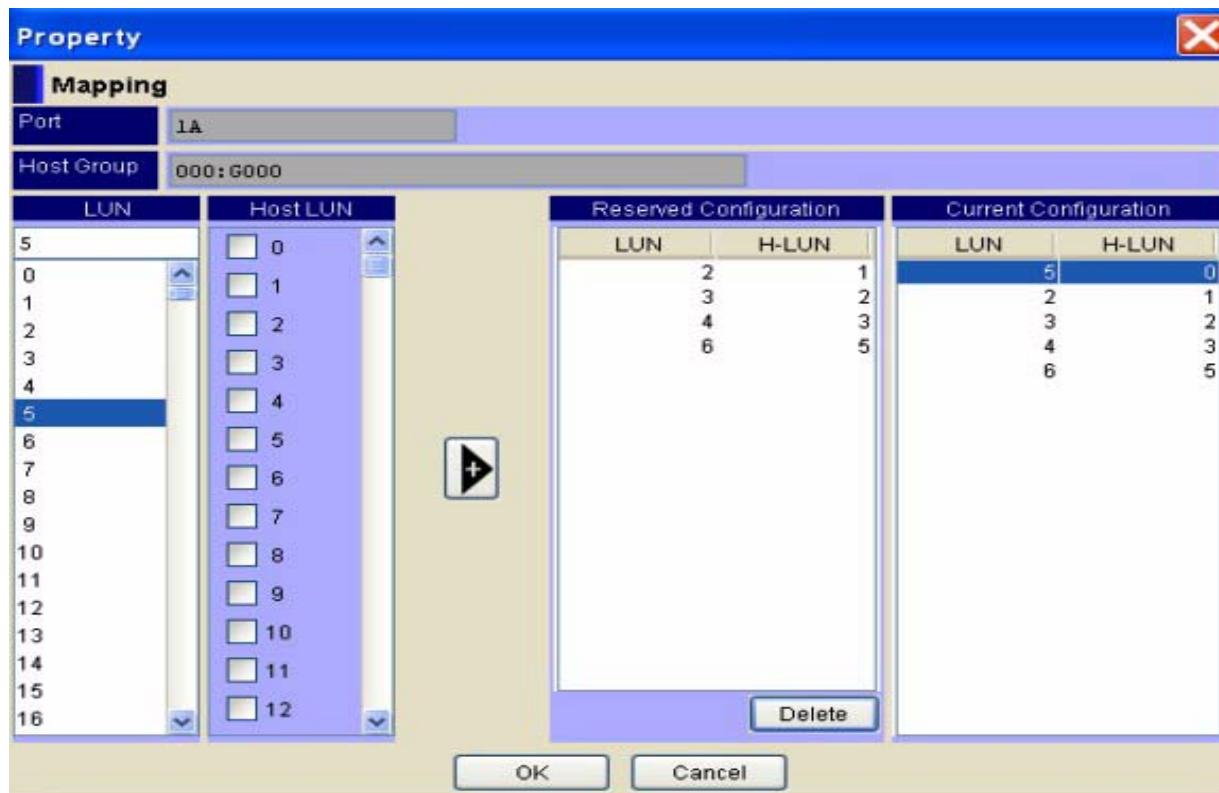
Figure 8-13 *Modify Mapping*



A new window appears, which is where the LU mapping takes place on the Hitachi storage side.

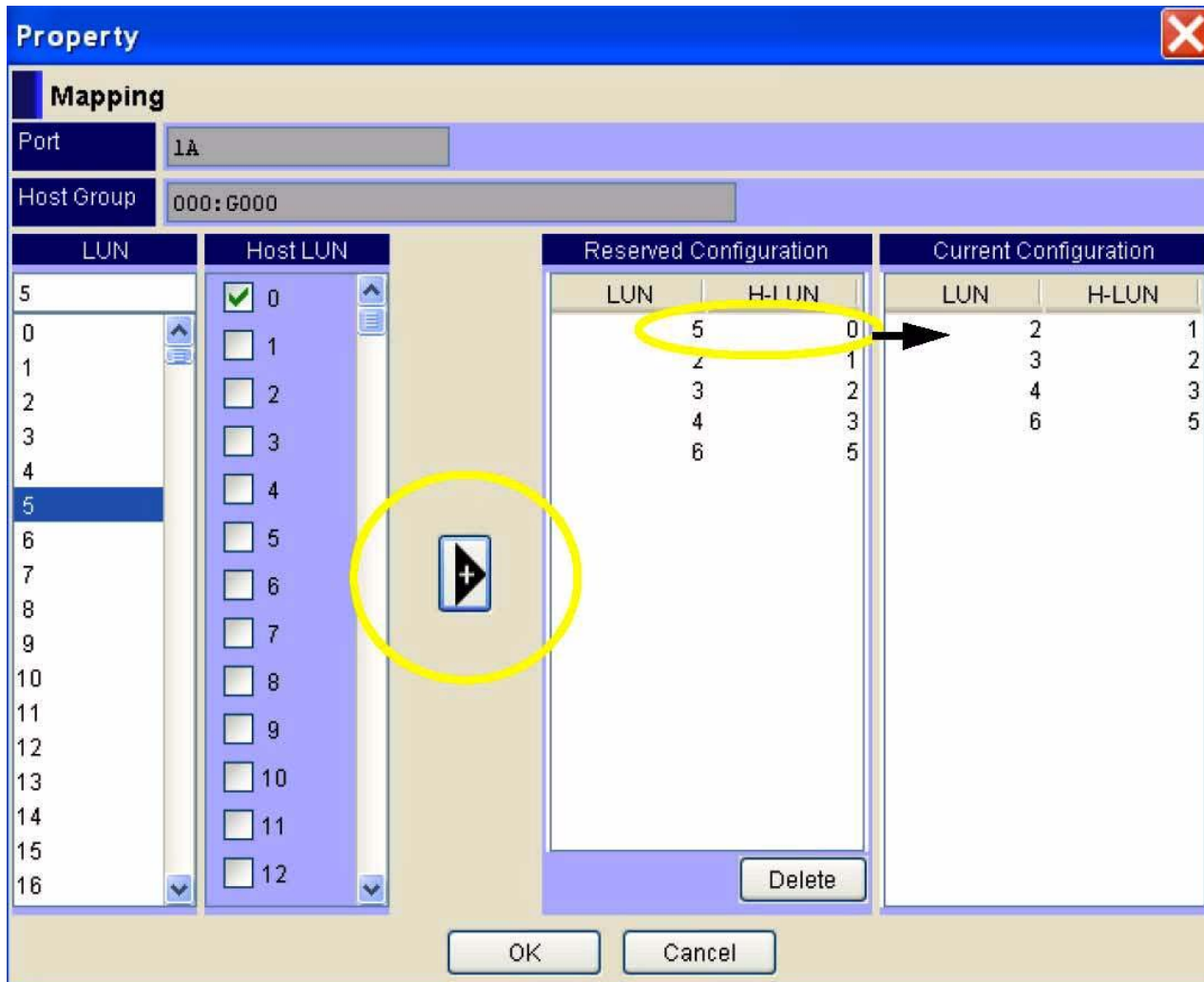
- Step 7** Select an LU to add from the LUN table. The LUN table contains all possible LUs on the array side. (See [Figure 8-14](#).)

Figure 8-14 Select a LUN and a Host LUN



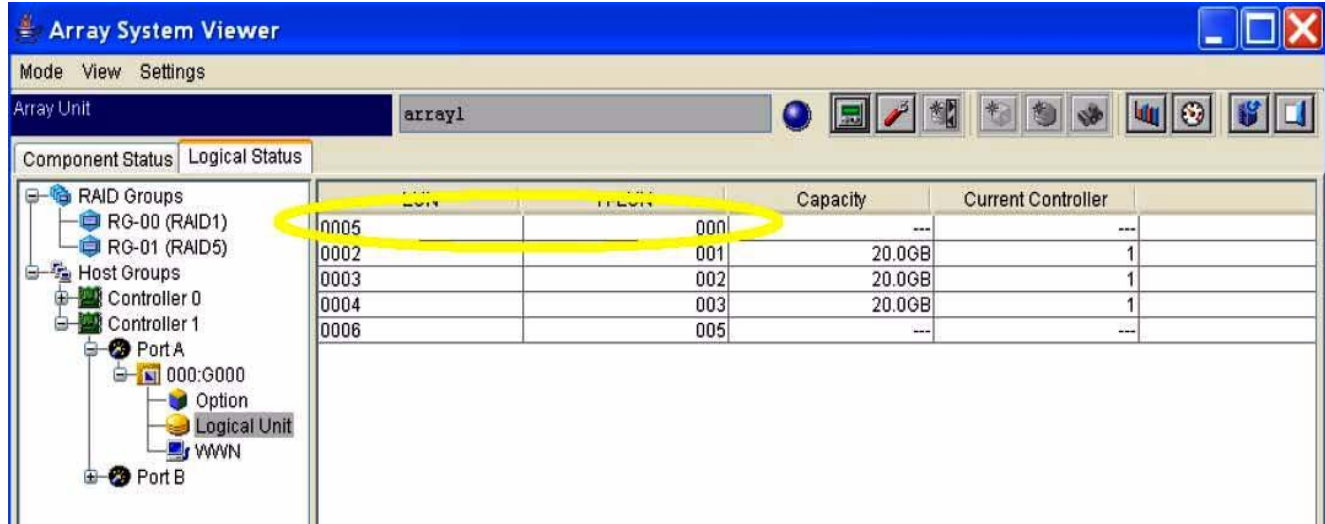
- Step 8** Select a host LUN from the Host LUN table. This option determines the LU number that is exported by the array for the LU that you selected from the first table. You must select a Host LUN, even if it is 0.
- Step 9** Add the LU mapping to the **Reserved Configuration** table.
- Click on the “+” sign in the middle of the window to add the LU to the Reserved Configuration table. The Reserved Configuration table contains the configuration that is applied after you click the **OK** button. (See [Figure 8-15](#).)
 - Repeat Step 9a for each LU that you want to map.

Figure 8-15 Add the LUNs to the Configuration Table

**Note**

The last table, which is the Current Configuration table, contains the active LU mapping on the array, which will change when you have completed the configuration.

- Step 10** Click **OK**. The configuration in the Reserved Configuration table becomes the Current Configuration. The new LUN mapping is added to the current active configuration. (See [Figure 8-16](#).) The LUN Mapping window closes.

Figure 8-16 New LUN in the Active Configuration

- Step 11** Use Element Manager or the CLI to discover LUNs for an initiator.
- Step 12** Use Element Manager or the CLI to verify that the LU(s) that you chose to be seen by this storage group are discovered.
- Step 13** If the LU(s) are not visible, verify that the LUN mapping has been applied to be the active configuration. If you are using Host Group Security, check the WWNs in the host group.
- Step 14** Repeat the LU mapping steps to map LUs through additional host groups or controller ports, as needed.



CHAPTER 9

LUN Remapping

The following sections appear in this chapter:

- [Introduction, page 9-1](#)
- [Creating an SRP LUN for a Fibre Channel LUN, page 9-1](#)
- [Configuration Example, page 9-3](#)

Introduction

To communicate with Fibre Channel storage, SRP hosts must access an LU that they map as “LUN 0.” By default, LUN 0 maps to the LU with a Fibre Channel LUN ID of 0 (00:00:00:00:00:00:00:00). If you want a host to access certain LUs in a storage device, but you want to deny that host access to LUN 0, you must map another LU to serve as LUN 0 for that host.

Creating an SRP LUN for a Fibre Channel LUN

You can perform this process with the CLI, with Element Manager, or with Chassis Manager.

Using the CLI

To map a Fibre Channel LUN to an SRP LUN, enter the **fc srp itl** command with the following:

- the GUID of the host
- the GUID extension of the host
- the WWPN of the target
- the Fibre Channel LUN ID of the LU
- the **srp-lunid** keyword
- the LUN ID (LUN 0) that you want to apply to the LU
- the **logical-id** keyword
- the logical ID of the LU that you want to map to SRP LUN 0

to map the Fibre Channel LUN to the SRP LUN.

[illegible]

Using Chassis Manager

To map a Fibre Channel LUN to an SRP LUN, perform the following steps:

- | | |
|---------------|--|
| Step 1 | Launch your Web browser, and enter the IP address of your switch in the address bar to start Chassis Manager. |
| Step 2 | Expand the Fibre Channel icon, and then click the ITLs branch. |
| Step 3 | Click the radio button next to the ITL that you want to remap, and then click the Properties button. The SRP ITL Properties window opens. |
| Step 4 | In the SRP LUN ID field, enter the LUN ID that you want the SRP host to map to the Logical ID of the LU. |
| Step 5 | Click the Apply button, and then click the Close button. |

Using Element Manager



Note

The instructions in this section assume that you have connected hardware and discovered LUNs.

To map a Fibre Channel LUN to an SRP LUN, perform the following steps:

- Step 1** Launch Element Manager, and open the server switch that connects your host to your storage.
- Step 2** From the FibreChannel menu, select **Storage Manager**. The Storage Manager window opens.

- Step 3** Expand the SRP Hosts folder and click a host to which you want to deny access to the LU that maps to Fibre Channel LUN ID 00:00:00:00:00:00:00:00.
- Step 4** Click the **LUN Access** tab.
- Step 5** If you have not done so already, click the LUN(s), in the Available LUNs field, to which you want to grant your host access, then click the **Add >** button. The LUN moves from the **Available LUNs** field to the **Accessible LUNs** field.
- Step 6** Click the **Apply** button.
- Step 7** Click the LUN, in the Accessible LUNs field, that you want to remap, and then click the **Edit ITL Properties** button. The **ITL Properties** window opens.
- Step 8** In the **SRP LUN ID** field, enter the new LUN that you want your host to use to identify the LU, and then click the **Apply** button.

**Note**

You must not use the same LUN to map to multiple LUs. Verify that your SRP host does not already use the LUN that you want to assign to identify another LU.

- Step 9** Click the **Close** button.

Configuration Example

The instructions in this section explain how to configure three hosts that connect, through a server switch, to one Fibre Channel RAID device so that each host accesses different LUs, and no two hosts can access the same LU(s). In this scenario, the following points apply:

- Host 1 can access the LU with Fibre Channel LUN ID 00:00:00:00:00:00:00:00.
- Hosts 2 and 3 cannot access the LU with Fibre Channel LUN ID 00:00:00:00:00:00:00:00.
- Host 1 must access LUs with non-sequential Fibre Channel LUN IDs.
- All hosts already have full access to the LUs that they need, so you only need to remove access, not grant additional access.

- Step 1** Launch Element Manager and open the server switch that connects the IB hosts to the Fibre Channel storage.
- Step 2** From the FibreChannel menu, select **Storage Manager**.
- Step 3** Expand the **SRP Hosts** folder and click Host 1.
- Step 4** Click the **LUN Access** tab.
- Step 5** Expand the gateway and target icons in the Accessible LUNs field to display the LUs.
- Step 6** Hold the **Ctrl** key and click each LU that you do not want Host 1 to access, then click the **<Remove** button. The LUs move from the Accessible LUNs field to the Available LUNs field.
- Step 7** Click the first LU in the Accessible LUNs field, then click the **Edit ITL Properties** button.
- Step 8** Verify that the Fibre Channel LUN ID field displays **00:00:00:00:00:00:00:00**.
- Step 9** Verify that the SRP LUN ID field displays **00:00:00:00:00:00:00:00**.
- Step 10** Close the window and click the next LU in the **Accessible LUNs** field.

- Step 11** Verify that the SRP LUN ID field displays **00:00:00:00:00:00:00:01**. If the field displays another value, change the value to **00:00:00:00:00:00:00:01** and click the **Apply** button.
- Step 12** Repeat Step 10 and Step 11 for each LU in the Accessible LUNs field and, for each LU, increment the SRP LUN ID by 1 (in hexadecimal notation).
- Step 13** In the SRP Hosts folder, click **Host 2**.
- Step 14** Hold the **Ctrl** key and click each LU that you do not want Host 2 to access, then click the **<Remove** button. The LUs move from the Accessible LUNs field to the Available LUNs field.
- Step 15** Click the first LU in the Accessible LUNs field, then click the **Edit ITL Properties** button.
- Step 16** Change the value in the SRP LUN ID field to **00:00:00:00:00:00:00:00**.
- Step 17** Continue down the list of LUs in the Accessible LUNs field and increment the **SRP LUN ID** value for each LU by 1 (in hexadecimal notation).
- Step 18** Repeat Step 13 through Step 17 for Host 3.
-



CHAPTER 10

Monitoring Storage Traffic

The following sections appear in this chapter:

- [Introduction](#)
- [Global Statistics, page 10-1](#)
- [SRP/FCP Statistics, page 10-4](#)
- [Fibre Channel Gateway Statistics, page 10-4](#)
- [Viewing ITL Statistics, page 10-5](#)

Introduction

You can monitor storage statistics with Element Manager to audit and troubleshoot your system. The Element Manager Statistics window displays the following:

- network and performance statistics for SRP ITLs
- SRP/FCP traffic statistics across the gateways of all the Fibre Channel cards
- SRP/FCP traffic statistics across the gateways of an individual Fibre Channel card

Global Statistics

Global statistics represent the aggregate total of all SRP/FCP traffic statistics across the gateways of all Fibre Channel interface card.

Global Tab Field Descriptions

The columns in the Global tab are described in [Table 10-1](#).

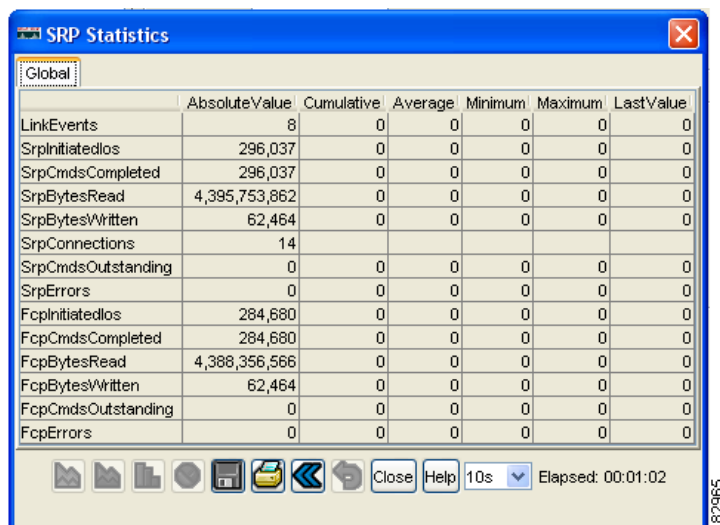
Table 10-1 Global Tab Field Descriptions

Field	Description
LinkEvents	Total number of link events processed by the Fibre Channel interface gateway.
SrpInitiatedIos	Number of I/O transactions that were initiated by the SRP host.
SrpCmdsCompleted	Total number of SRP commands completed on the Fibre Channel interface gateway.
SrpBytesRead	Number of bytes read by the SRP initiator.
SrpBytesWritten	Number of bytes written by the SRP initiator.
SrpConnections	Number of connections maintained by the SRP initiator.
SrpCmdsOutstanding	Total number of SRP commands outstanding on the Fibre Channel interface gateway.
SrpErrors	Total number of SRP errors encountered on the Fibre Channel interface gateway.
FcpInitiatedIos	Number of I/O transactions that were initiated by the Fibre Channel device.
FcpCmdsCompleted	Total number of FCP commands completed on the Fibre Channel interface gateway.
FcpBytesRead	Number of bytes read by the Fibre Channel device.
FcpBytesWritten	Number of bytes written by the Fibre Channel device.
FcpCmdsOutstanding	Total number of FCP commands outstanding on the Fibre Channel interface gateway.
FCPErrors	Total number of FCP errors encountered on the Fibre Channel interface gateway.

Viewing Global Statistics

To view the SRP and FCP global traffic statistics, perform the following steps:

-
- Step 1** Launch Element Manager.
 - Step 2** From the Fibre Channel menu, select **Storage Manager**. The Cisco Storage Manager window opens.
 - Step 3** Click the **Statistics** folder in the Storage navigation tree. Statistics fields appear in the right-hand display.
 - Step 4** Click the **Graph Global Statistics** button in the Global Statistics portion of the display. The **SRP Statistics** window opens and displays the Global tab. (See [Figure 10-1](#).)

Figure 10-1 SRP Statistics Window: Global Tab

Note The pulldown menu in the lower-right-hand corner of [Figure 10-1](#) assigns a refresh rate to the graph.

Step 5 Click-and-drag to select the statistics that you want to graph. The various graph buttons become available. (See [Figure 10-2](#).)

Figure 10-2 Graph Buttons

a.	b.	c.	d.
----	----	----	----

- a. line chart
- b. area chart
- c. bar chart
- d. pie chart

Step 6 Click the button of the graph that you want to create.

SRP/FCP Statistics

The FC-4 protocol for the serial SCSI command protocol is used on Fibre Channel networks.

Viewing SRP/FCP Statistics

To view SRP/FCP statistics, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Launch Element Manager. |
| Step 2 | From the Fibre Channel menu, select Storage Manager . The Cisco Storage Manager window opens. |
| Step 3 | Click the Statistics folder in the Storage navigation tree. The Storage Manager window gives you the option to view these statistics: <ul style="list-style-type: none">• Global statistics.• Gateway statistics.• ITL statistics. |
-

Fibre Channel Gateway Statistics

Gateway statistics represent the total SRP/FCP traffic across the gateway of an individual Fibre Channel interface card.

Viewing Statistics for a Specific Gateway

To view the statistics for a specific Fibre Channel gateway, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Launch Element Manager. |
| Step 2 | From the FibreChannel menu, select Storage Manager . The Cisco Storage Manager window opens. |
| Step 3 | Click the Statistics folder in the Storage navigation tree. Statistics fields appear in the right-hand display. |
| Step 4 | Click a Fibre Channel gateway card in the Gateways field of the Gateway Statistics portion of the display. |
| Step 5 | Click the Graph Gateway Statistics button. The SRP Statistics window opens and displays a single tab for the gateway that you selected. (See Figure 10-3 .) |

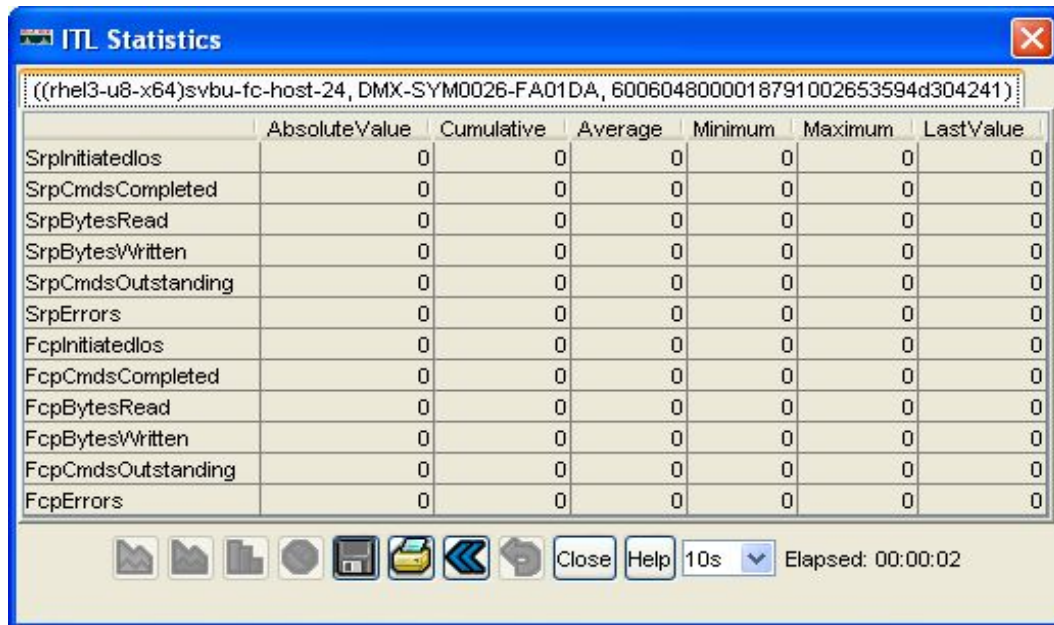
Figure 10-3 SRP Statistics Window: Card (Gateway) Tab

	AbsoluteValue	Cumulative	Average	Minimum	Maximum	LastValue
LinkEvents	4	0	0	0	0	0
SrpInitiatedIos	160,487	0	0	0	0	0
SrpCmdsCompleted	160,487	0	0	0	0	0
SrpBytesRead	4,335,045,951	0	0	0	0	0
SrpBytesWritten	16,384	0	0	0	0	0
SrpConnections	7					
SrpCmdsOutstanding	0	0	0	0	0	0
SrpErrors	0	0	0	0	0	0
FcpInitiatedIos	152,044	0	0	0	0	0
FcpCmdsCompleted	152,044	0	0	0	0	0
FcpBytesRead	4,334,760,574	0	0	0	0	0
FcpBytesWritten	16,384	0	0	0	0	0
FcpCmdsOutstanding	0	0	0	0	0	0
FcpErrors	0	0	0	0	0	0

Viewing ITL Statistics

To view the statistics of an initiator, target, and LUN on a specific gateway card, perform the following steps:

- Step 1** Launch Element Manager.
- Step 2** From the FibreChannel menu, select **Storage Manager**. The Cisco Storage Manager window opens.
- Step 3** Click the **Statistics** folder in the Storage navigation tree. Statistics fields appear in the right-hand display.
- Step 4** From the **Initiator** pulldown menu in the ITL Statistics portion of the display, select the initiator of the ITL whose statistics you want to view.
- Step 5** From the Target pulldown menu in the ITL Statistics portion of the display, select the target of the ITL whose statistics you want to view.
- Step 6** From the LUN pulldown menu in the ITL Statistics portion of the display, select the LUN of the ITL whose statistics you want to view.
- Step 7** From the Gateway pulldown menu in the ITL Statistics portion of the display, select a gateway over which the ITL runs. The output will display ITL statistics for that gateway only.
- Step 8** Click the **Graph ITL Statistics** button. The ITL Statistics window opens and displays a name at the top. (See [Figure 10-4](#).) The name is comprised of the selected initiator, target service name, and LUN. For a description of this window and its fields, refer to the [“Global Statistics” section on page 10-1](#).

Figure 10-4 ITL Statistics

Step 9 Select the type of data to graph by selecting the appropriate table cell.

Step 10 Select the type of graph to display. The graph appears.



INDEX

A

access
 LUN [5-27](#)
 port [3-3, 5-21](#)
access control [1-5](#)
audience [vii](#)
auto-bind [1-2, 5-19](#)

B

bandwidth [1-4](#)

C

conventions, document [viii](#)

D

defaults [1-3, 5-2](#)
device
 random [1-3](#)
 sequential [1-3](#)
Discover LUNs [5-8, 5-10](#)
document
 audience [vii](#)
 conventions [viii](#)
 organization [vii](#)
 related [ix](#)
dynamic path affinity [3-6](#)
dynamic port failover [3-8](#)

F

failover
 about [1-5](#)
 configuring [3-2](#)
failover, gateway [2-3](#)
FCP statistics [10-3](#)
features
 failover [1-5](#)
 hardware [1-4](#)
 high availability [1-5](#)
 load balancing [1-5](#)
 path affinity [1-5](#)
 redundancy [1-5, 2-1](#)
 software [1-4](#)

G

gateway failover [2-3](#)
global attributes [3-1](#)
global policies [3-1](#)
global statistics [10-1](#)
granting port access [3-9](#)

H

hardware features [1-4](#)
high availability [1-5](#)
hi mark [3-2, 3-4](#)

I

I/O hi mark [3-2, 3-4](#)

I/O timeout [3-6](#)
 initiator [1-2, 1-8](#)
 initiator, target, LUN (ITL) [1-3](#)
 install [4-1](#)
 ITL [1-3](#)
 ITLs
 configuring [5-7](#)
 ITLs, configuring individually [5-32](#)
 ITs [1-3, 5-21](#)

L

LEDs [4-2](#)
 load balancing [3-7](#)
 about [1-5](#)
 configuring [3-2](#)
 logical unit [1-3](#)
 logical unit number [1-3](#)
 LU [1-3](#)
 LUN [1-3, 1-9](#)
 LUN access [5-27](#)
 access
 LUN [3-3](#)
 configuring [3-8, 3-9](#)
 restricting (CLI) [3-9](#)
 restricting (GUI) [3-2, 3-3](#)
 LUN masking [1-6](#)
 configuring [3-8, 3-9](#)

M

maintenance [1-4](#)
 maximum retries [3-5](#)
 minimum I/O timeout [3-6](#)

O

organization, document [vii](#)

P

path affinity [1-3, 3-6](#)
 about [1-5](#)
 configuring [3-2](#)
 port access [3-3, 5-21](#)
 configuring [3-9, 3-10](#)
 granting [3-9](#)
 restricting (CLI) [3-10](#)
 restricting (GUI) [3-2, 3-3, 3-4](#)
 port failover [3-8](#)
 port load balancing [3-7](#)
 port masking [1-6](#)
 configuring [3-9, 3-10](#)

R

random device [1-3](#)
 recovery [2-3](#)
 redistributing connections [2-4](#)
 redundancy [1-5](#)
 redundant topologies [2-1](#)
 related documentation [ix](#)

S

sequential device [1-3](#)
 service name [1-3](#)
 software features [1-4](#)
 speed [1-4, 1-6](#)
 SRP host [1-3](#)
 SRP statistics [10-3](#)
 statistics
 FCP [10-3](#)
 SRP [10-3](#)
 statistics, global [10-1](#)

T

target [1-3, 1-9](#)

topologies, redundant [2-1](#)

topology emulation [1-3](#)

transparent topology emulation [1-3](#)

Z

zoning [1-6](#)